การเปรียบเทียบจุดอ่อนต่อการโจมตีในเซิร์ฟเวอร์โดยใช้ซีวีอี

นายไกรสีห์ อัญชนานนท์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2548

ISBN 974-53-2466-3

COMPARISON ON VULNERABILITIES TO ATTACK AGAINST SERVERS BY USING CVE

Mr. Kraisie Anchananon

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science Program in Computer Science

Department of Computer Engineering

Faculty of Engineering

Chulalongkorn University

Academic Year 2005

ISBN 974-53-2466-3

หัวข้อวิทยานิพนธ์	การเปรียบเทียบจุดอ่อนต่อการโจมตีในเซิร์ฟเวอร์โดยใช้ซีวีอี
โดย	นายไกรสีห์ อัญชนานนท์
สาขาวิชา	วิทยาศาสตร์คอมพิวเตอร์
อาจารย์ที่ปรึกษา	อาจารย์ ดร. ยรรยง เต็งอำนวย

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดีคณะวิศวกรรมศาสตร์

(ศาสตราจารย์ ดร. ดิเรก ลาวัณย์ศิริ)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ

(อาจารย์ ธงชัย โรจนกังสดาล)

..... อาจารย์ที่ปรึกษา

(อาจารย์ ดร. ยรรยง เต็งอำนวย)

..... กรรมการ

(นาย ชยา ลิมจิตติ)

.....กรรมการ

(นางสาว รัศมีทิพย์ วิตา)

ไกรสีห์ อัญชนานนท์ : การเปรียบเทียบจุดอ่อนต่อการโจมตีในเซิร์ฟเวอร์โดยใช้ซีวีอี
(COMPARISON ON VULNERABILITIES TO ATTACK AGAINST SERVERS BY USING CVE)
อ. ที่ปรึกษา : อ. ดร. ยรรยง เต็งอำนวย, 105 หน้า. ISBN 974-53-2466-3.

จุดอ่อนที่เกิดขึ้นในระบบคอมพิวเตอร์มักถูกนำมาใช้เป็นช่องทางสำคัญในการโจมตีของผู้ที่ไม่หวังดีเพื่อสร้างความเสียหายต่อระบบ ทำให้ระบบคอมพิวเตอร์ไม่สามารถให้บริการต่อไปได้ หรือเพื่อมุ่งหวังข้อมูลสำคัญที่มีอยู่ในระบบ ความเสียหายดังกล่าวนอกจากจะส่งผลกระทบต่อการทำงานของผู้ใช้งานแล้ว ยังอาจส่งผลกระทบต่อธุรกิจที่มีมูลค่ามหาศาลได้

จากปัญหาดังกล่าวทำให้เกิดแนวความคิดในการเปรียบเทียบจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์ประเภทต่างๆ ว่ามีความเปราะบางหรือมีความเสี่ยงต่อการถูกโจมตีมากน้อยเพียงใด ซึ่งจะเป็นประโยชน์โดยเฉพาะอย่างยิ่งกับผู้ดูแลระบบ สามารถใช้เป็นข้อมูลเบื้องต้นเพื่อช่วยในการตัดสินใจเลือกนำเซิร์ฟเวอร์มาใช้ในองค์กรและสามารถนำมาเปรียบเทียบสำหรับเซิร์ฟเวอร์ที่มีใช้งานอยู่แล้ว ว่าควรเพิ่มมาตรการป้องกันหรือแก้ไขจุดอ่อนใดบ้าง เพื่อทำให้เซิร์ฟเวอร์มีความแข็งแกร่งมากขึ้น และลดอัตราเสี่ยงต่อความเสียหายที่อาจเกิดขึ้นจากการถูกโจมตีได้

ผลของงานวิจัยที่ได้จากการจัดกลุ่มจุดอ่อนที่มีการรวบรวมไว้ในรายการซีวีอี ตั้งแต่ปี ค.ศ. 1999 ถึง ค.ศ.2004 และวิเคราะห์ความเปราะบางที่เกิดขึ้น สรุปผลได้ว่า เซิร์ฟเวอร์ที่มีจุดอ่อนและความเสี่ยงต่อการถูกโจมตีสูงได้แก่เซิร์ฟเวอร์ที่ให้บริการบนเครือข่ายอินเทอร์เน็ตที่มีการเข้าถึงจากกลุ่มผู้ใช้งานเป็นจำนวนมาก เช่น เว็บแอพพลิเคชั่นเซิร์ฟเวอร์, เว็บเซิร์ฟเวอร์, เมล์เซิร์ฟเวอร์ เป็นต้น และระบบปฏิบัติการที่ได้รับผลกระทบจากจุดอ่อนเป็นจำนวนมากที่สุด ได้แก่ ระบบปฏิบัติการบนแพลตฟอร์มวินโดวส์

ภาควิชา....วิศวกรรมคอมพิวเตอร์..... ลายมือชื่อนิสิต.....
สาขาวิชา...วิทยาศาสตร์คอมพิวเตอร์..... ลายมือชื่ออาจารย์ที่ปรึกษา.....
ปีการศึกษา. 2548.....

4671403621 : MAJOR COMPUTER SCIENCE

KEY WORD: CVE / TAXONOMY / VULNERABILITY / SERVER

KRAISIE ANCHANANON: COMPARISON ON VULNERABILITIES TO ATTACK AGAINST SERVERS BY USING CVE. THESIS ADVISOR: YUNYONG TENG-AMNUAY, Ph.D., 105 pp. ISBN 974-53-2466-3.

Vulnerabilities in computer systems are normally used as a means to destroy the systems by ill wishers; attempting either to break down services available or to get access to restricted important areas in the systems. Those destructive effects place damages not only to the work of users, but also to that of high valued businesses.

The above problems lead to the thought of creating comparisons on vulnerabilities generated by various kinds of servers, as to how much they are susceptible to and risky of attacks. This will, in particular, benefit system administrators as a primary source in decision making to select optimal servers for use in their organizations. Also, it will enable them to balance pros and cons of the servers currently in house, whether they would need more protection or any vulnerability correction. With these being carried out, the servers in question would be strongly and securely guarded. Additionally, risky rates to damages from the attacks would be decreased.

Evidently, the research's output in which vulnerabilities are grouped and listed in the 1999-2004 CVE descriptions, including analyses of vulnerabilities occurred, it can be concluded that servers which are most prone to vulnerabilities and vastly risky to attacks are those offering services on the Internet; for example, web application servers, web servers and mail servers that can be accessed by a large number of end-users. Besides, Operating System which are mostly affected by vulnerabilities are the ones on Windows Platforms

Department.... Computer Engineering..... Student's signature.....

Field of study.. Computer Science..... Advisor's signature.....

Academic year.. 2005.....

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้ด้วยดีโดยได้รับความกรุณาเป็นอย่างยิ่งจาก อาจารย์ ดร. ยรรยง เต็งอำนวย อาจารย์ที่ปรึกษา ที่ได้กรุณาสละเวลาให้คำปรึกษาแนะนำตลอดระยะเวลาในการทำวิทยานิพนธ์ฉบับนี้ จึงใคร่ขอกราบขอบพระคุณอาจารย์เป็นอย่างสูงไว้ ณ ที่นี้ด้วย

ขอขอบคุณ คุณชนะ ปรีชามานิตกุล คุณพรทิพย์ มาลีลัย และคุณเสาวลักษณ์ รัตนธรรมสกุล เพื่อนๆร่วมรุ่น CT14 สำหรับความช่วยเหลือในทุกๆเรื่อง รวมถึงคำปรึกษาและกำลังใจที่มีให้กันเสมอ

ขอขอบพระคุณ คุณแม่ และครอบครัว ที่คอยให้กำลังใจ ส่งเสริมในเรื่องการศึกษา ให้การสนับสนุนในทุกๆเรื่องตลอดมา และอยู่เคียงข้างในยามที่ผิดหวังและท้อแท้ ตั้งแต่เด็กจนถึงปัจจุบันและตลอดไป

ขอขอบคุณทุกๆกำลังใจที่ทำให้ผู้เขียนสามารถฝ่าฟันอุปสรรคต่างๆจนทำงานวิจัยสำเร็จลุล่วงลงได้ด้วยดี

สารบัญ

หน้า

บทคัดย่อภาษาไทย ..... ง
บทคัดย่อภาษาอังกฤษ ..... จ
กิตติกรรมประกาศ ..... ฉ
สารบัญ ..... ช
สารบัญตาราง ..... ฌ
สารบัญภาพ ..... ญ
บทที่
1 บทนำ 1
1.1 ความเป็นมาและความสำคัญของปัญหา 1
1.2 วัตถุประสงค์ของการวิจัย 2
1.3 ขอบเขตของการวิจัย 2
1.4 ขั้นตอนการวิจัย 3
1.5 ประโยชน์ที่คาดว่าจะได้รับ 4
1.6 โครงสร้างวิทยานิพนธ์ 4
2 ทฤษฎีและงานวิจัยที่เกี่ยวข้อง 5
2.1 Common Vulnerabilities and Exposures (CVE) 5
2.2 ทฤษฎีที่เกี่ยวข้องกับการจัดกลุ่มของจุดอ่อน 7
2.2.1 งานวิจัย “ A Taxonomy of Computer Program Security Flaws ” 8
2.2.2 งานวิจัย “ การประเมินและเปรียบเทียบการป้องกันจุดอ่อนของระบบลินุกซ์โดยการเพิ่มความแข็งแกร่งกับการใช้แอลเอสเอ็ม ” 10
2.3 ทฤษฎีที่เกี่ยวข้องกับการประเมินผลจุดอ่อน 10
2.3.1 งานวิจัย " การประเมินความเสี่ยงเว็บเซิร์ฟเวอร์โดยการจำแนกระดับผลกระทบของความเสียหาย " 10
2.3.2 งานวิจัย “Maintaining Software with a Security Perspective” 11
2.3.3 งานวิจัย “Assessing computer security vulnerability” 11
3 การคัดเลือกและการจัดเก็บข้อมูลจุดอ่อน 13
3.1 การคัดเลือกข้อมูลจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์จากรายการซีวีอี 13
3.2 การจัดกลุ่มจุดอ่อน 19
3.3 โครงสร้างตารางจัดเก็บข้อมูล 21

บทที่ หน้า

3.4 ตัวอย่างตารางการจัดเก็บข้อมูล 27
4 การนับจำนวนและคำนวณคะแนนความเปราะบางจากข้อมูลจุดอ่อน 31
4.1 การนับจำนวนจุดอ่อน 31
4.2 การคำนวณคะแนนความเปราะบางจากจุดอ่อน 32
4.3 ตัวอย่างการคำนวณคะแนนความเปราะบางจากข้อมูลจุดอ่อน 39
5 ผลการวิจัย 45
5.1 ตารางแจกแจงผลลัพธ์ที่ได้ 47
5.2 ประเมินและเปรียบเทียบจุดอ่อนและความเปราะบางต่อการโจมตีบนเซิร์ฟเวอร์ ... 54
5.2.1 ประเมินและเปรียบเทียบจุดอ่อนที่เกิดขึ้นกับเซิร์ฟเวอร์ประเภทต่างๆ 55
5.2.2 ประเมินและเปรียบเทียบความเปราะบางต่อการโจมตีของเซิร์ฟเวอร์ประเภทต่างๆ 61
5.2.3 ประเมินและเปรียบเทียบจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์ของระบบปฏิบัติการประเภทต่างๆ 71
5.2.4 ประเมินและเปรียบเทียบความเปราะบางต่อการโจมตีบนเซิร์ฟเวอร์ของระบบปฏิบัติการประเภทต่างๆ 83
6 สรุปผลการวิจัยและข้อเสนอแนะ 100
6.1 สรุปผลการวิจัย 100
6.2 ข้อเสนอแนะ 102
6.3 งานวิจัยในอนาคต 103
รายการอ้างอิง 104
ประวัติผู้เขียนวิทยานิพนธ์ 105

สารบัญตาราง

ตารางที่ หน้า

2.1 แสดงการอ้างอิงจุดอ่อนที่เกิดขึ้นกับโปรแกรมซีจีไอของสมุดโทรศัพท์พีเอชเอฟของหน่วยงานต่างๆ 5
3.1 แสดงตัวอย่างข้อมูลจุดอ่อนในรายการซีวีอี ซึ่งประกอบไปด้วยหมายเลขซีวีอี คำอธิบาย และแหล่งข้อมูลอ้างอิง 14
3.2 แสดงรายชื่อแหล่งข้อมูลจุดอ่อนต่างๆ 15
3.3 แสดงตัวอย่างรายละเอียดของแหล่งข้อมูลจุดอ่อนต่างๆ 15
3.4 รูปแบบตารางการเก็บข้อมูลของระบบปฏิบัติการ.....23
3.5 แสดงตัวอย่างตารางการจัดเก็บข้อมูลจุดอ่อนที่เกิดขึ้นบน Database Server 29
4.1 ตารางการให้คะแนนจุดอ่อน 34
5.1 สรุปจำนวนจุดอ่อนที่เกิดขึ้นโดยแบ่งแยกตามการจัดกลุ่มจุดอ่อน, ระบบปฏิบัติการที่ได้รับผลกระทบ และปีที่เกิดจุดอ่อนนั้นๆ 48
5.2 ตัวอย่างตารางแจกแจงจุดอ่อนของเซิร์ฟเวอร์ตามระบบปฏิบัติการเทียบกับประเภทของจุดอ่อนที่เกิดขึ้นในปี 1999 49
5.3 ตัวอย่างตารางแจกแจงจุดอ่อนของเซิร์ฟเวอร์ตามระบบปฏิบัติการเทียบกับจุดที่เกิดจุดอ่อนและระดับความรุนแรงที่เกิดขึ้นในปี 1999 50
5.4 ตัวอย่างตารางแจกแจงคะแนนความเปราะบางของเซิร์ฟเวอร์ตามประเภทของจุดอ่อนที่เกิดขึ้นในปี 1999 51
5.5 ตัวอย่างตารางแจกแจงคะแนนความเปราะบางของเซิร์ฟเวอร์ตามจุดที่เกิดจุดอ่อนที่เกิดขึ้นในปี 1999 51
5.6 ตัวอย่างตารางแจกแจงคะแนนความเปราะบางของเซิร์ฟเวอร์ตามระบบปฏิบัติการที่ได้รับผลกระทบที่เกิดขึ้นในปี 1999 52
5.7 แสดงรายชื่อเซิร์ฟเวอร์ที่มีจุดอ่อนและคะแนนความเปราะบางมาที่สุด 5 อันดับแรก 61
5.8 ตารางคะแนนความเปราะบางของเซิร์ฟเวอร์เมื่อเทียบประเภทของจุดอ่อนและลักษณะความเสียหายที่เกิดขึ้น 67
5.9 ตารางคะแนนความเปราะบางของเซิร์ฟเวอร์เมื่อเทียบจุดที่เกิดจุดอ่อนและลักษณะความเสียหายที่เกิดขึ้น 70
5.10 ตารางคะแนนความเปราะบางของเซิร์ฟเวอร์เมื่อเทียบระบบปฏิบัติการและลักษณะความเสียหายที่เกิดขึ้น 92

สารบัญภาพ

รูปที่ หน้า

2.1 แสดงแนวความคิดของการใช้ซีวีอีเพื่ออ้างอิงรายการจุดอ่อนที่เกิดขึ้น ……..... 6

2.2 แสดงตัวอย่างข้อมูลจุดอ่อนที่ปรากฏในรายการซีวีอี 7

2.3 การแบ่งกลุ่มข้อบกพร่องของ Lanwehr โดยแบ่งออกตามลักษณะการเกิดของข้อบกพร่อง....8

2.4 การแบ่งกลุ่มข้อบกพร่องของ Lanwehr โดยแบ่งออกตามเวลาที่เกิดของข้อบกพร่อง ……. 9

2.5 การแบ่งกลุ่มข้อบกพร่องของ Lanwehr โดยแบ่งออกตามสถานที่ที่เกิดของข้อบกพร่อง 9

3.1 แสดงรายละเอียดของแหล่งข้อมูลจุดอ่อน XF ……16

3.2 เว็บไซต์ของ X-Force Vulnerability Database ……..……16

3.3 แสดงผลตัวอย่างการหาข้อมูลของรหัสอ้างอิง sun-libnsl ……..17

3.4 ตัวอย่างรายละเอียดข้อมูลที่ได้จากการค้นหารหัสอ้างอิง sum-libnsl …….. 17

3.5 ภาพขยายของรูปที่ 3.4 ตัวอย่างรายละเอียดข้อมูลที่ได้จากการค้นหารหัสอ้างอิง sum-libnsl ……18

3.6 ตัวอย่างรายละเอียดข้อมูลจุดอ่อนของ CVE-2000-0004 ที่ค้นหาได้จากแหล่งข้อมูล XF ….19

3.7 แสดงแม่แบบตารางการจัดเก็บข้อมูลจุดอ่อน#1 ……... 25

3.8 แสดงแม่แบบตารางการจัดเก็บข้อมูลจุดอ่อน#2 ……..…… 25

3.9 แสดงแม่แบบตารางการจัดเก็บข้อมูลจุดอ่อน#3 ……..…… 26

3.10 แสดงแม่แบบตารางการจัดเก็บข้อมูลจุดอ่อน#4 …… 26

3.11 แสดงแม่แบบตารางการจัดเก็บข้อมูลจุดอ่อน#5 …… 27

4.1 กระบวนการคัดเลือกข้อมูลจุดอ่อนและเตรียมข้อมูลเพื่อนำไปใช้ในการคำนวณผลต่างๆ ….35

4.2 ตัวอย่างข้อมูลจุดอ่อนที่จัดเก็บในตารางบนฐานข้อมูลของตัวอย่างตารางที่ 3.5#1 …… 37

4.3 ตัวอย่างข้อมูลจุดอ่อนที่จัดเก็บในตารางบนฐานข้อมูลของตัวอย่างตารางที่ 3.5#2 …… 37

4.4 ตัวอย่างข้อมูลจุดอ่อนที่จัดเก็บในตารางบนฐานข้อมูลของตัวอย่างตารางที่ 3.5#3 …… 38

4.5 ตัวอย่างข้อมูลจุดอ่อนที่จัดเก็บในตารางบนฐานข้อมูลของตัวอย่างตารางที่ 3.5#4 …… 38

4.6 ตัวอย่างการแปลงโครงสร้างรูปแบบหัวตารางจากตารางในแฟ้มข้อมูลเอ็กซ์เซลเป็นตารางในฐานข้อมูล ……..……39

5.1 แสดงเว็บเพจสำหรับใช้สืบค้นข้อมูลจำนวนจุดอ่อนและคะแนนความเปราะบางของเซิร์ฟเวอร์ 46

5.2 กราฟเปรียบเทียบจำนวนจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์กับจำนวนจุดอ่อนในรายการซีวีอี …53

5.3 กราฟแสดงอัตราส่วนเป็นร้อยละของจำนวนจุดอ่อนบนเซิร์ฟเวอร์เมื่อเทียบกับจำนวนจุดอ่อนในรายการซีวีอี 54

รูปที่ หน้า

5.4 กราฟแสดงจำนวนรายการจุดอ่อนบนเซิร์ฟเวอร์แต่ละประเภทเรียงตามชื่อของเซิร์ฟเวอร์ 56
5.5 กราฟแสดงจำนวนรายการจุดอ่อนบนเซิร์ฟเวอร์แต่ละประเภทเรียงตามจำนวนจุดอ่อน 57
5.6 กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์แยกตามประเภทจุดอ่อนและปีที่เกิดจุดอ่อน 58
5.7 กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์แยกตามประเภทจุดอ่อน 58
5.8 กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์แยกตามจุดที่เกิดจุดอ่อนและปีที่เกิดจุดอ่อน 59
5.9 กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์แยกตามจุดที่เกิดจุดอ่อน 59
5.10 กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์แยกตามลักษณะความเสียหายและปีที่เกิด
จุดอ่อน 60
5.11 กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์แยกตามลักษณะความเสียหาย 60
5.12 กราฟแสดงคะแนนความเปราะบางต่อการโจมตีบนเซิร์ฟเวอร์เรียงตามชื่อของเซิร์ฟเวอร์ ...63
5.13 กราฟแสดงคะแนนความเปราะบางต่อการโจมตีบนเซิร์ฟเวอร์เรียงตามคะแนน 64
5.14 กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์แยกตามประเภทของจุดอ่อนและปีที่
เกิดจุดอ่อน 65
5.15 กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์แยกตามประเภทของจุดอ่อน.....66
5.16 กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์แยกตามจุดที่เกิดจุดอ่อนและปีที่เกิด
จุดอ่อน 68
5.17 กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์แยกตามจุดที่เกิดจุดอ่อน.....69
5.18 กราฟแสดงอัตราส่วนร้อยละของความเปราะบางบนเซิร์ฟเวอร์ตามจุดที่เกิดจุดอ่อน 69
5.19 กราฟเปรียบเทียบจำนวนจุดอ่อนของเซิร์ฟเวอร์บนระบบปฏิบัติการต่างๆ#1 73
5.20 กราฟเปรียบเทียบจำนวนจุดอ่อนของเซิร์ฟเวอร์บนระบบปฏิบัติการต่างๆ#2 74
5.21 กราฟเปรียบเทียบจำนวนจุดอ่อนของเซิร์ฟเวอร์บนระบบปฏิบัติการต่างๆ#3 75
5.22 กราฟเปรียบเทียบจำนวนจุดอ่อนของเซิร์ฟเวอร์บนระบบปฏิบัติการต่างๆ#4 76
5.23 กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์ของระบบปฏิบัติการต่างๆ 77
5.24 กราฟแสดงอัตราส่วนร้อยละของจำนวนจุดอ่อนบนเซิร์ฟเวอร์ของระบบปฏิบัติการต่างๆ ...77
5.25 กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์ของระบบปฏิบัติการยูนิกซ์ 78
5.26 กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์ของระบบปฏิบัติการลินุกซ์ 78
5.27 กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์ของระบบปฏิบัติการวินโดวส์ 79
5.28 กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์ของระบบปฏิบัติการอื่นๆและที่ไม่มีการระบุไว้ใน
รายการอ้างอิง 79

รูปที่ หน้า

5.29 กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์แยกตามประเภทของระบบปฏิบัติการยูนิกซ์ และปีที่เกิดจุดอ่อน 80
5.30 กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์แยกตามประเภทของระบบปฏิบัติการลินุกซ์ และปีที่เกิดจุดอ่อน 81
5.31 กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์แยกตามประเภทของระบบปฏิบัติการวินโดวส์ และปีที่เกิดจุดอ่อน 82
5.32 กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์แยกตามประเภทของระบบปฏิบัติการอื่นๆ และปีที่เกิดจุดอ่อน 83
5.33 กราฟเปรียบเทียบคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการต่างๆ#1 86
5.34 กราฟเปรียบเทียบคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการต่างๆ#2 87
5.35 กราฟเปรียบเทียบคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการต่างๆ#3 88
5.36 กราฟเปรียบเทียบคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการต่างๆ#4 89
5.37 กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการประเภทต่างๆ 90
5.38 กราฟแสดงอัตราส่วนร้อยละของความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการ ประเภทต่างๆ 91
5.39 กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการยูนิกซ์ 93
5.40 กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการลินุกซ์ 93
5.41 กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการวินโดวส์ 94
5.42 กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการอื่นๆและที่ไม่มีการ ระบุไว้ในรายการอ้างอิง 94
5.43 กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการยูนิกซ์แยกตามปี ที่เกิดจุดอ่อน 95
5.44 กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการลินุกซ์แยกตามปี ที่เกิดจุดอ่อน 96
5.45 กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการวินโดวส์แยกตามปี ที่เกิดจุดอ่อน 97
5.46 กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการอื่นๆแยกตามปี ที่เกิดจุดอ่อน 98

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันในปัจจุบันคอมพิวเตอร์ได้เข้ามามีบทบาทต่อการทำงานเป็นอย่างมากสำหรับหน่วยงานต่างๆทั้งในภาครัฐและภาคเอกชน แต่ละองค์กรจึงจำเป็นต้องมีเซิร์ฟเวอร์(Server)ประเภทต่างๆเพื่อให้บริการผู้ใช้งานจากภายในและภายนอกองค์กร การพิจารณาเลือกเซิร์ฟเวอร์เพื่อนำมาใช้งานในองค์กร นอกเหนือจากการพิจารณาถึงเรื่องฮาร์ดแวร์(Hardware) ของเครื่องแล้ว แพลตฟอร์มและระบบปฏิบัติการรวมทั้งโปรแกรมประยุกต์ต่างๆที่ทำงานบนเครื่องเซิร์ฟเวอร์นั้นๆก็เป็นสิ่งที่ไม่ควรถูกมองข้ามเช่นกัน เพราะสิ่งต่างๆเหล่านี้อาจมีผลต่อการรักษาความปลอดภัยของระบบคอมพิวเตอร์ในองค์กรได้ ควรจะเลือกเซิร์ฟเวอร์อย่างไรจึงจะเหมาะสมและปลอดภัยจากการถูกโจมตีจากผู้ไม่หวังดีต่อระบบทั้งหลายซึ่งอาจจะมีอยู่ทั้งภายในและภายนอกองค์กรได้

จุดอ่อนที่มีปรากฏอยู่ในระบบคอมพิวเตอร์นับเป็นสิ่งหนึ่งที่ผู้ไม่หวังดีต่อระบบมักใช้เป็นช่องทางในการโจมตีและสร้างความเสียหายแก่ระบบ เช่น การบุกรุกล่วงละเมิดเข้าสู่ระบบ, การขโมยข้อมูลอันเป็นความลับ, การทำให้ระบบอยู่ในสภาพไม่พร้อมให้บริการ เป็นต้น มีงานวิจัยหลายชิ้นที่ได้พยายามทำการจัดกลุ่มให้แก่จุดอ่อนที่เกิดขึ้นในระบบคอมพิวเตอร์เหล่านี้ เช่น [1],[2] งานวิจัย [3] เป็นอีกหนึ่งงานวิจัยที่ได้มีการจัดกลุ่มของจุดอ่อนเพื่อทำการประเมินและเปรียบเทียบการป้องกันจุดอ่อนของระบบลินุกซ์ จากงานวิจัยดังกล่าวทำให้เกิดข้อสงสัยเกี่ยวกับการเกิดจุดอ่อนบนระบบปฏิบัติการต่างๆ ว่าจุดอ่อนที่เกิดขึ้นบนแต่ละระบบปฏิบัติการนั้นมีปริมาณมากน้อยต่างกันเพียงใด จุดอ่อนที่เกิดขึ้นดังกล่าวแม้เกิดขึ้นแต่เพียงเล็กน้อยก็อาจส่งผลกระทบที่รุนแรงต่อระบบคอมพิวเตอร์ได้ โดยเฉพาะ อย่างยิ่งการโจมตียังเซิร์ฟเวอร์ที่ให้บริการต่างๆ ซึ่งปริมาณจุดอ่อนที่เกิดขึ้นย่อมแสดงให้เห็นถึงอัตราเสี่ยงและความเปราะบางต่อการโจมที่เกิดขึ้นได้

งานวิจัยนี้จึงมีแนวความคิดที่จะวิเคราะห์และเปรียบเทียบให้เห็นถึงความเปราะบางต่อการโจมตีของเซิร์ฟเวอร์ประเภทต่างๆ โดยพิจารณาจากข้อมูลจุดอ่อนที่ได้มีการรวบรวมไว้ในรายการซีวีอี[4] ซึ่งจะนำมาแบ่งประเภทตามกลุ่มของจุดอ่อนและระบบปฏิบัติการที่ได้รับผลกระทบต่อจุดอ่อนนั้น ซึ่งจะเป็นประโยชน์ต่อการพิจารณาเลือกเซิร์ฟเวอร์ประเภทนั้นๆ ให้สามารถนำมาใช้ในองค์กรได้อย่างเหมาะสม รวมถึงเป็นข้อมูลพื้นฐานเพื่อนำไปใช้ในการหาแนวทางการป้องกันสำหรับเซิร์ฟเวอร์ที่มีใช้อยู่แล้วในองค์กร เพื่อเป็นการช่วยลดความเสี่ยงต่อการถูกโจมตีและป้องกันความเสียหายที่อาจเกิดขึ้นได้

1.2 วัตถุประสงค์ของการวิจัย

เพื่อวิเคราะห์และเปรียบเทียบจุดอ่อนของเซิร์ฟเวอร์บนแพลตฟอร์มของระบบปฏิบัติการที่แตกต่างกัน

1.3 ขอบเขตของการวิจัย

1. ใช้ซีวีอีเวอร์ชัน 20040901 ซึ่งมีรายการอยู่ทั้งหมด 3,053 รายการ โดยเลือกเฉพาะรายการจุดอ่อนที่เกิดขึ้นบนซอฟต์แวร์เซิร์ฟเวอร์ ซึ่งได้แก่จุดอ่อนที่เกิดขึ้นกับซอฟต์แวร์และโปรแกรมประยุกต์ต่างๆที่ทำงานบนซอฟต์แวร์เซิร์ฟเวอร์ โดยซอฟต์แวร์เซิร์ฟเวอร์ในที่นี้หมายถึงโปรแกรมประยุกต์ซึ่งทำหน้าที่ให้บริการบนแพลตฟอร์มของระบบปฏิบัติการบนเครื่องคอมพิวเตอร์

2. เซิร์ฟเวอร์ที่พิจารณาในงานวิจัยนี้ประกอบไปด้วย เซิร์ฟเวอร์ทั้งหมด 29 ชนิด ได้แก่

2.1 Access Control Server (ACS)

2.2 Application Server

2.3 Cache Server

2.4 Chat Server

2.5 Cluster Server

2.6 Database Server

2.7 DHCP(Dynamic Host Configuration Protocol) Server

2.8 DNS(Domain Name System) Server

2.9 Finger Server

2.10 FTP(File Transfer Protocol) Server

2.11 Game Server

2.12 Gopher Server

2.13 INN(InterNetNews) Server

2.14 Kerberos Server

2.15 LDAP(Lightweight Directory Access Protocol) Server

2.16 Mail Server

2.17 Multimedia Server

2.18 NFS(Network File System) Server

2.19 NIS(Network Information Service) Server

2.20 PKI(Public Key Infrastructure) Server

2.21 Proxy Server

2.22 Radius Server

2.23 SNMP(Simple Network Management Protocol) Server

2.24 Telnet Server

2.25 Terminal Server

2.26 Time Server

2.27 Web Server

2.28 Web Application Server

2.29 WINS(Windows Internet Naming Service) Server

1.4 ขั้นตอนการวิจัย

1. ศึกษาโครงสร้างและข้อมูลซีวีอี

2. คัดเลือกรายการจุดอ่อนจากรายการซีวีอีโดยเลือกเฉพาะรายการจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์

3. สร้างตารางแจกแจงข้อมูลรายละเอียดของจุดอ่อน โดยแบ่งออกเป็นหัวข้อหลักๆ ดังนี้

3.1 รายการจุดอ่อน

3.2 กลุ่มของจุดอ่อน

3.3 ประเภทของเซิร์ฟเวอร์

3.4 ประเภทของระบบปฏิบัติการที่ได้รับผลกระทบจากจุดอ่อน

4. แจกแจงรายการจุดอ่อนแต่ละรายการออกตามกลุ่มของจุดอ่อน, ประเภทของเซิร์ฟเวอร์ เช่น Web Server, FTP Server, Mail Server, Proxy Server เป็นต้น และประเภทของระบบปฏิบัติการที่ได้รับผลกระทบจากจุดอ่อน จากข้อมูลที่ค้นหาได้จากเว็บไซต์ต่างๆตามรายการอ้างอิงที่มีระบุไว้ในซีวีอีและเว็บไซต์(Web Site)อื่นๆ เช่น [5], [6], [7], [8], [9]

5. ทำการให้คะแนนแก่จุดอ่อนแต่ละรายการ

6. สรุปคะแนนที่ได้ของเซิร์ฟเวอร์แต่ละประเภท โดยแยกตามกลุ่มของจุดอ่อนและระบบปฏิบัติการที่ได้รับผลกระทบจากจุดอ่อน

7. ทำการประเมินและเปรียบเทียบ ความเปราะบางของเซิร์ฟเวอร์ของระบบปฏิบัติการประเภทต่างๆ

8. สรุปผลการดำเนินงานวิจัยและจัดทำรายงานวิทยานิพนธ์

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1. รายการจุดอ่อนทั้งหมดของเซิร์ฟเวอร์แต่ละประเภท สามารถนำข้อมูลรายการจุดอ่อนต่างๆเหล่านั้นเป็นข้อมูลพื้นฐานเพื่อใช้ในการหาวิธีการป้องกันเซิร์ฟเวอร์จากการโจมตีของผู้ไม่หวังดีต่อระบบได้

2. สามารถนำข้อมูลจากงานวิจัยไปใช้เป็นข้อมูลช่วยสนับสนุนในการตัดสินใจเลือกใช้เซิร์ฟเวอร์แต่ละ ประเภทสำหรับองค์กร โดยสามารถเปรียบเทียบความปลอดภัยจากการโจมตีจุดอ่อนของเซิร์ฟเวอร์บนระบบปฏิบัติการแพลตฟอร์มต่างๆ

1.6 โครงสร้างวิทยานิพนธ์

ในบทที่ 2 จะกล่าวถึงทฤษฎีและงานวิจัยที่เกี่ยวข้อง บทที่ 3 จะกล่าวถึงการคัดเลือกและการจัดเก็บข้อมูลจุดอ่อน รวมถึงโครงสร้างตารางจัดเก็บข้อมูล บทที่ 4 จะกล่าวถึงการคำนวณคะแนนความเปราะบางจากจุดอ่อน พร้อมทั้งยกตัวอย่างการคำนวณคะแนนดังกล่าว บทที่ 5 จะเป็นผลงานวิจัย ซึ่งเป็นผลที่ได้จากการเปรียบเทียบและการประเมินจุดอ่อนที่เกิดขึ้นและความเปราะบางบนเซิร์ฟเวอร์ประเภทต่างๆ และทำการสรุปผลที่ได้รวมถึงข้อเสนอแนะต่างๆไว้ในบทที่ 6

บทที่ 2

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

ทฤษฎีและงานวิจัยที่เกี่ยวข้องที่จำเป็นต้องศึกษาเพื่อใช้เป็นความรู้พื้นฐานในการทำงานวิจัยนี้ แบ่งออกได้เป็น 3 ส่วนด้วยกัน อันประกอบไปด้วย จุดอ่อนที่เกิดขึ้นในระบบคอมพิวเตอร์ โดยศึกษาจากข้อมูลรายการจุดอ่อนที่มีปรากฏอยู่ในรายการซีวีอี, การจัดกลุ่มของจุดอ่อน และการประเมินผลจุดอ่อน ดังรายละเอียดต่อไปนี้

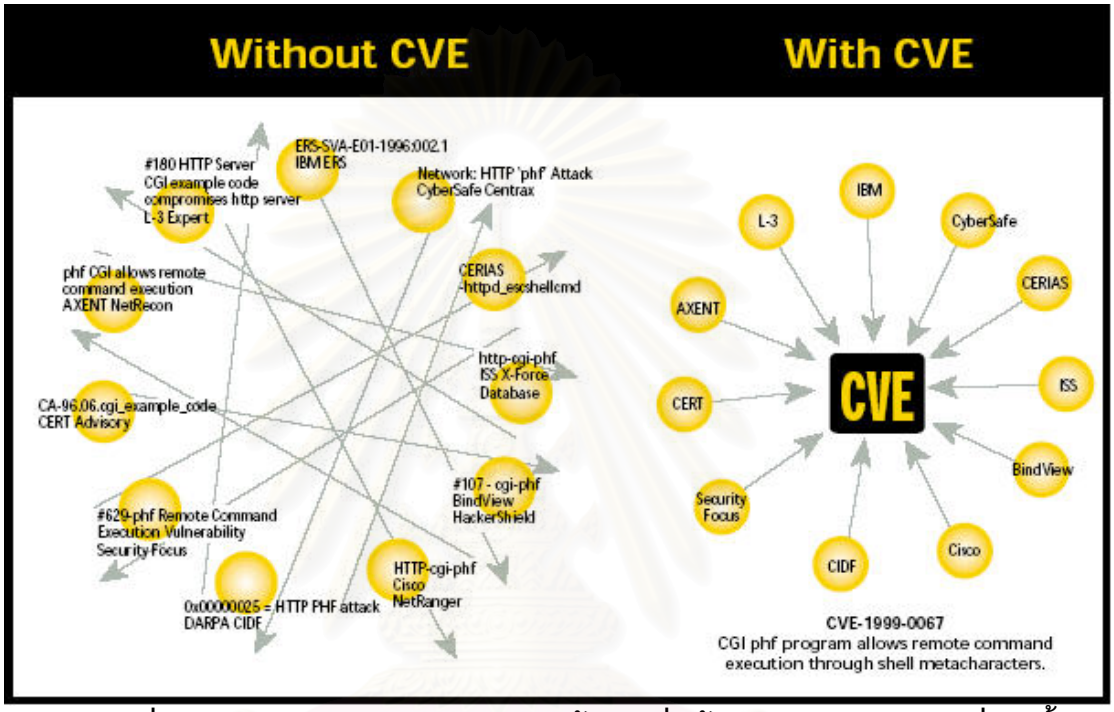
2.1 Common Vulnerabilities and Exposures (CVE)

ซีวีอี (Common Vulnerability and Exposure (CVE)) [10] เป็นการกำหนดชื่อที่เป็นมาตรฐานของรายการจุดอ่อนที่เกิดขึ้นในระบบคอมพิวเตอร์ ซึ่งแต่เดิมจุดอ่อนที่เกิดขึ้นในระบบคอมพิวเตอร์มักจะถูกกำหนดชื่อเรียกแตกต่างกันออกไป ตามองค์กรหรือหน่วยงานที่แตกต่างกัน เช่น การอ้างอิงจุดอ่อนที่เกิดขึ้นกับโปรแกรมซีจีไอของสมุดโทรศัพท์พีเอชเอฟ ในปี 1998 ดังรายละเอียดในตารางที่ 2.1

Organization	Name referring to vulnerability
AXENT(now Symantec)	phf CGI allows remote command execution
BindView	#107—cgi-phf
Bugtraq	PHF Attacks—fun and games for the whole family
CERIAS	http_escshellcmd
CERT	CA-96.06.cgi_example_code
Cisco Systems	HTTP—cgi-phf
CyberSafe	Network: HTTP ‘phf’ attack
DARPA	0x00000025 = HTTP PHF attack
IBM ERS	ERS-SVA-E01-1996:002.1
ISS	http—cgi-phf
Symantec	#180 HTTP server CGI example code compromises http server
SecurityFocus	#629—phf Remote Command Execution Vulnerability

ตารางที่ 2.1 แสดงการอ้างอิงจุดอ่อนที่เกิดขึ้นกับโปรแกรมซีจีไอของสมุดโทรศัพท์พีเอชเอฟของหน่วยงานต่าง ๆ

จากสาเหตุนี้เองจึงทำให้การทำความเข้าใจต่อจุดอ่อนที่เกิดขึ้น การเลือกใช้เครื่องมือป้องกันจุดอ่อนที่เหมาะสม และการอ้างอิงถึงจุดอ่อนรายการเดียวกันจากหน่วยงานที่แตกต่างกันเป็นไปด้วยความยากลำบาก ซีวีอีจึงถูกกำหนดขึ้นสำหรับแก้ปัญหาที่เกิดขึ้นนี้ เพื่อลดความขัดแย้งในการอ้างอิงถึงจุดอ่อนที่เกิดขึ้นทางด้านความปลอดภัยและสร้างความเป็นมาตรฐานให้กับจุดอ่อนต่างๆที่เกิดขึ้นในระบบคอมพิวเตอร์



รูปที่ 2.1 แสดงแนวความคิดของการใช้ซีวีอีเพื่ออ้างอิงรายการจุดอ่อนที่เกิดขึ้น

จากรูปที่ 2.1 การอ้างอิงถึงรายการจุดอ่อนระหว่างหน่วยงานต่างๆแต่เดิมทำได้ยาก เนื่องจากแต่ละหน่วยงานมักจะมีการอ้างอิงรายการจุดอ่อนโดยใช้ชื่อที่แต่ละหน่วยงานนั้นๆเป็นผู้กำหนดขึ้น ทำให้การติดต่อสื่อสารกับหน่วยงานอื่นเมื่อต้องการอ้างถึงจุดอ่อนรายการเดียวกันเป็นเรื่องที่ยุ่งยากซับซ้อนโดยเฉพาะอย่างยิ่งเมื่อต้องการติดต่อกับหน่วยงานอื่นมากกว่า 2 หน่วยงานขึ้นไป การนำซีวีอีมาใช้ทำให้มีการอ้างรายการจุดอ่อนผ่านชื่อที่มีความเป็นมาตรฐาน ทำให้การอ้างอิงถึงรายการจุดอ่อนเดียวกันของแต่ละหน่วยงานทำได้ง่ายมากยิ่งขึ้น

ข้อมูลจุดอ่อนที่ปรากฏอยู่ในรายการซีวีอี มีองค์ประกอบอยู่ 3 ส่วน ด้วยกัน ได้แก่

1. ชื่อรายการจุดอ่อน (Name) เป็นการตั้งชื่อเพื่อให้เป็นมาตรฐานในการอ้างอิงถึงข้อมูลจุดอ่อน โดยมีรูปแบบดังนี้ CAN-YYYY-NNNN โดย CAN บอกให้รู้ว่าเป็นหมายเลขแคนดิเดต(Candidate) YYYY เป็นปีที่ออกหมายเลขแคนดิเดต และ NNNN คือ ลำดับที่ของแคนดิเดตที่ออกในปีนั้น ซึ่งหากแคนดิเดตนั้นได้รับการ

ยอมรับและผ่านการพิจารณาจาก Editorial Board ก็จะถูกเพิ่มรายการลงในรายการซีวีอี พร้อมทั้งเปลี่ยนชื่อจาก CAN-YYYY-NNNN เป็น CVE-NNNN-YYYY เช่น CAN-2000-1001 เป็น CVE-2000-1001

2. คำอธิบาย (Description) จะเป็นคำอธิบายสั้นๆถึงจุดอ่อนที่เกิดขึ้นนั้นว่าเป็นจุดอ่อนที่เกี่ยวข้องกับเรื่องใด

3. แหล่งข้อมูลอ้างอิง (References) จะบอกถึงแหล่งข้อมูลอื่นๆที่สามารถนำไปใช้ในการค้นหาข้อมูลรายละเอียดของจุดอ่อนนั้นๆเพิ่มเติมได้

CVE Name	Description	Reference
CVE-2000-1001	add_2_basket.asp in Element InstantShop allows remote attackers to modify price information via the "price" hidden form variable.	BUGTRAQ:20001024 Price modification in Element InstantShop,XF:instantshop-modify-price,OSVDB:6487

รูปที่ 2.2 แสดงตัวอย่างข้อมูลจุดอ่อนที่ปรากฏในรายการซีวีอี

จากรูปที่ 2.2 จะแสดงตัวอย่างของข้อมูลจุดอ่อนในรายการซีวีอี พร้อมทั้งรูปแบบการตั้งชื่อ คำอธิบายและการอ้างอิงถึงแหล่งข้อมูลอ้างอิงต่างๆ

2.2 ทฤษฎีที่เกี่ยวข้องกับการจัดกลุ่มของจุดอ่อน

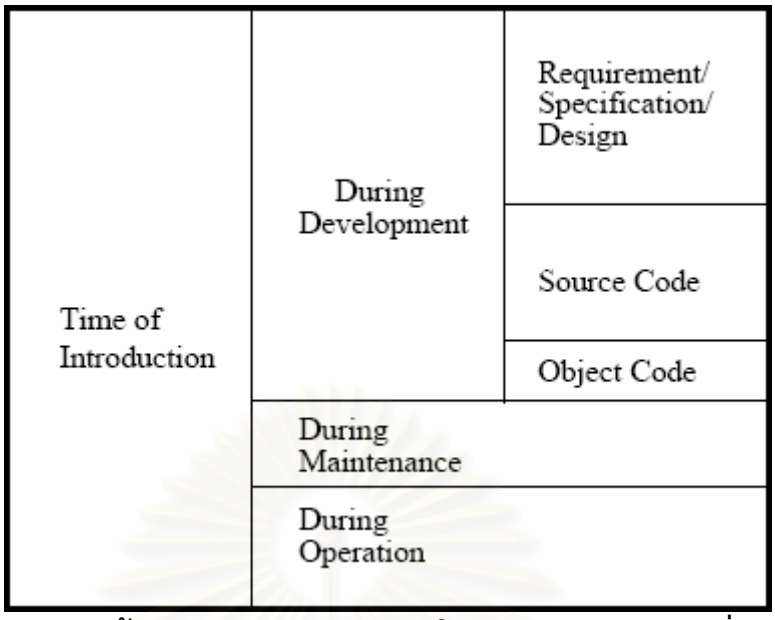
เนื่องจากงานวิจัยนี้ต้องการเปรียบเทียบจุดอ่อนต่อการโจมตีในเซิร์ฟเวอร์ โดยจุดอ่อนที่เกิดขึ้นนั้นย่อมมีลักษณะที่แตกต่างกันออกไปไม่เหมือนกัน เช่น จุดอ่อนนั้นเกิดขึ้นได้อย่างไร เกิดขึ้น ณ ที่ใด และจุดอ่อนนั้นก่อให้เกิดความเสียหายอย่างไรแก่ระบบได้บ้าง เป็นต้น ดังนั้นจึงจำเป็นต้องศึกษาทฤษฎีหรืองานวิจัยที่เกี่ยวข้องกับจุดอ่อนว่า จุดอ่อนที่เกิดขึ้นในระบบคอมพิวเตอร์นั้นมีลักษณะเป็นอย่างไรบ้าง สามารถที่จะจัดกลุ่มหรือแบ่งหมวดหมู่ของจุดอ่อนที่เกิดขึ้นเหล่านั้นได้หรือไม่ โดยจากการศึกษาพบว่ามีงานวิจัยที่เกี่ยวข้องที่น่าสนใจอยู่ 2 งานวิจัย ที่กล่าวถึงการจัดกลุ่มของจุดอ่อนหรือข้อบกพร่องที่เกิดขึ้น ซึ่งมีรายละเอียดดังต่อไปนี้

2.2.1 งานวิจัย “ A Taxonomy of Computer Program Security Flaws ”

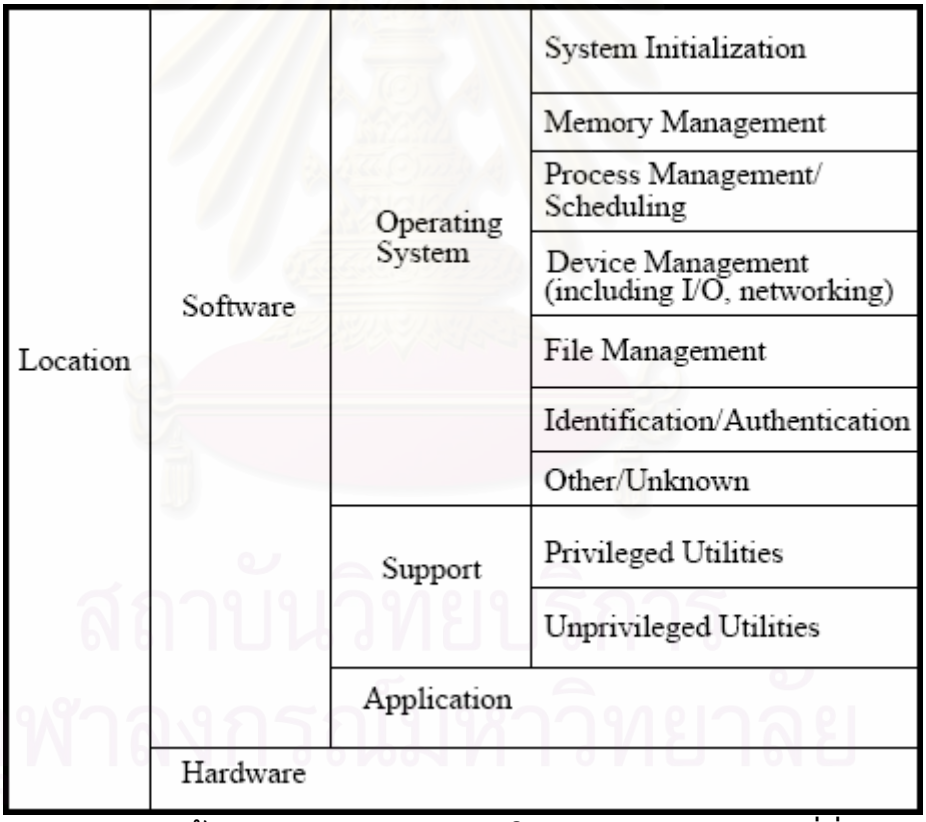
Lanwehr และคณะ [1] ได้จัดกลุ่มของข้อบกพร่องในด้านความปลอดภัยของโปรแกรมคอมพิวเตอร์ตามลักษณะความคล้ายคลึงกันของข้อบกพร่องที่เกิดขึ้น โดยแบ่งข้อบกพร่องออกเป็น 3 กลุ่มตาม ลักษณะการเกิดของข้อบกพร่อง, เวลาที่เกิดข้อบกพร่องและสถานที่ที่เกิดข้อบกพร่อง

<table>
<tr><td rowspan="8">Genesis</td><td rowspan="6">Intentional</td><td rowspan="3">Malicious</td><td rowspan="2">Trojan Horse</td><td>Non-Replicating</td></tr>
<tr><td>Replicating (virus)</td></tr>
<tr><td colspan="2">Trapdoor</td></tr>
<tr><td colspan="2">Logic/Time Bomb</td></tr>
<tr><td rowspan="3">Nonmalicious</td><td rowspan="2">Covert Channel</td><td>Storage</td></tr>
<tr><td>Timing</td></tr>
<tr><td colspan="2">Other</td></tr>
<tr><td rowspan="5">Inadvertent</td><td colspan="3">Validation Error (Incomplete/Inconsistent)</td></tr>
<tr><td colspan="3">Domain Error (Including Object Re-use, Residuals, and Exposed Representation Errors)</td></tr>
<tr><td colspan="3">Serialization/aliasing (Including TOCTTOU Errors)</td></tr>
<tr><td colspan="3">Identification/Authentication Inadequate</td></tr>
<tr><td colspan="3">Boundary Condition Violation (Including Resource Exhaustion and Violable Constraint Errors)</td></tr>
<tr><td colspan="3">Other Exploitable Logic Error</td></tr>
</table>

รูปที่ 2.3 การแบ่งกลุ่มข้อบกพร่องของ Lanwehr โดยแบ่งออกตามลักษณะการเกิดของข้อบกพร่อง



รูปที่ 2.4 การแบ่งกลุ่มข้อบกพร่องของ Lanwehr โดยแบ่งออกตามเวลาที่เกิดข้อบกพร่อง



รูปที่ 2.5 การแบ่งกลุ่มข้อบกพร่องของ Lanwehr โดยแบ่งออกตามสถานที่ที่เกิดข้อบกพร่อง

จากรูปที่ 2.3 – 2.5 แสดงโครงสร้างการแบ่งกลุ่มข้อบกพร่องของ Lanwehr ออกตามปัจจัยต่างๆในการเกิดข้อบกพร่องนั้น โดยในรูปที่ 2.3 เป็นการแบ่งกลุ่มข้อบกพร่องออกตามลักษณะการเกิดของข้อบกพร่อง ซึ่งแบ่งออกได้กว้างๆคือ เป็นข้อบกพร่องอันเกิดจากเจตนามุ่งร้าย

ต่อระบบ เช่น ม้าโทรจัน และเป็นข้อบกพร่องที่เกิดขึ้นโดยไม่ได้ตั้งใจ เช่น ข้อบกพร่องต่อการตรวจสอบข้อมูลนำเข้าเป็นต้น ในรูปที่ 2.4 เป็นการแบ่งกลุ่มข้อบกพร่องออกตามเวลาที่เกิดข้อบกพร่อง ซึ่งจะแบ่งออกได้เป็น 3 ช่วงเวลา คือ ในช่วงระหว่างการพัฒนา ระหว่างการบำรุงรักษาและระหว่างการปฏิบัติการ ในรูปที่ 2.5 เป็นการแบ่งกลุ่มข้อบกพร่องออกตามสถานที่ที่เกิดข้อบกพร่อง โดยแยกออกเป็นข้อบกพร่องที่เกิดขึ้นบนส่วนของซอฟต์แวร์ (ซึ่งได้แก่ ระบบปฏิบัติการ โปรแกรมสนับสนุนการทำงานของระบบปฏิบัติการ และแอพพลิเคชัน) และฮาร์ดแวร์

2.2.2 งานวิจัย " การประเมินและเปรียบเทียบการป้องกันจุดอ่อนของระบบลินุกซ์โดยการเพิ่มความแข็งแกร่งกับการใช้แอลเอสเอ็ม "

งานวิจัยของรัศมีทิพย์ วิตา [3] เป็นการวิเคราะห์ความสามารถในการป้องกันการโจมตีบนระบบลินุกซ์หลังจากเสริมความปลอดภัยให้กับระบบลินุกซ์โดยการเพิ่มความแข็งแกร่งให้กับระบบและการใช้แอลเอสเอ็ม ในงานวิจัยนี้มีการจัดกลุ่มของจุดอ่อนที่เกิดขึ้น โดยเป็นการเสริมการจัดกลุ่มของจุดอ่อนของ Lanwehr [1] งานวิจัยนี้ได้แบ่งจุดอ่อนออกเป็น 4 รูปแบบ คือ ประเภทของจุดอ่อน, จุดที่เกิดจุดอ่อน, ลักษณะความเสียหาย และระดับความรุนแรง เพื่อทำการประเมินผลและเปรียบเทียบความสามารถในการป้องกันจุดอ่อนโดยใช้ค่าดัชนีความเปราะบางที่มีพื้นฐานการให้คะแนนจากจุดอ่อนที่เกิดขึ้นและการจัดประเภทของจุดอ่อน

2.3 ทฤษฎีที่เกี่ยวข้องกับการประเมินผลจุดอ่อน

เมื่อได้ศึกษางานวิจัยในการจัดกลุ่มของจุดอ่อนแล้ว เพื่อให้สามารถใช้ข้อมูลที่รวบรวมได้ นำมาวิเคราะห์และประเมินผลจุดอ่อนที่เกิดขึ้นรวมถึงความเปราะบางของเซิร์ฟเวอร์จึงจำเป็นต้องศึกษางานวิจัยเพิ่มเติมเพื่อหาแนวทางในการประเมินผลข้อมูลที่ได้รวมทั้งรูปแบบในการประเมินผล ซึ่งงานวิจัยทีเกี่ยวข้องมีรายละเอียดดังต่อไปนี้

2.3.1 งานวิจัย " การประเมินความเสี่ยงเว็บเซิร์ฟเวอร์โดยการจำแนกระดับผลกระทบของความเสียหาย "

งานวิจัยของเกียรติ ภิรมย์โสภา [11] งานวิจัยนี้ได้เสนอแนวทางในการประเมินความเสี่ยงของเว็บเซอร์เวอร์โดยการพิจารณาจากข้อมูลจุดอ่อนตามรายการซีวีอี และมีการวัดระดับผลกระทบของจุดบกพร่องที่สามารถคำนวณได้โดยการใช้ผลรวมคะแนนของระดับความเสียหายแต่ละประเภทที่เกิดขึ้น ได้แก่ การรักษาความลับ(Confidentiality), การบูรณภาพ(Integrity) และสภาพพร้อมใช้งาน(Availability) จากสมการ

$$Wi = Wc_i + WI_i + WA_i$$

โดยที่ Wi คือ ระดับผลกระทบของจุดบกพร่องใดๆ

Wc_i คือ ระดับผลกระทบของจุดบกพร่องใดๆ ที่ส่งผลต่อการรักษาความลับ

WI_i คือ ระดับผลกระทบของจุดบกพร่องใดๆ ที่ส่งผลต่อการบูรณภาพ

WA_i คือ ระดับผลกระทบของจุดบกพร่องใดๆ ที่ส่งผลต่อสภาพพร้อมใช้งาน

i คือ ลำดับของซีวีอี

โดยให้ค่าของผลกระทบที่ส่งผลต่อการรักษาความลับ(C) ผลกระทบที่ส่งผลต่อการรักษาบูรณภาพ(I) และผลกระทบที่ส่งผลต่อสภาพพร้อมใช้งาน(A) แต่ละประเภทมีค่าเป็น 1 และระดับของผลกระทบที่ได้แบ่งเป็น 3 ระดับ คือ ส่งผลกระทบสูง มีคะแนนเท่ากับ 3 ส่งผลกระทบปานกลาง มีคะแนนเท่ากับ 2 และส่งผลกระทบต่ำ มีคะแนนเท่ากับ 1แล้วจึงคำนวณโดยใช้สมการ $\sum_{i=1}^{n} W_i$ เพื่อคำนวณคะแนนผลกระทบโดยรวมของจุดบกพร่องออกมา

2.3.2 งานวิจัย “Maintaining Software with a Security Perspective”

Jiwnani และคณะ [2] ได้เสนอกลวิธีในการทดสอบซอร์ฟแวร์โดยมีพื้นฐานจากจุดอ่อนที่เกิดขึ้นเพื่อนำมาพัฒนาระบบที่มีความปลอดภัยและเสถียรภาพมากขึ้น โดยงานวิจัยนี้จะอาศัยหลักการจัดกลุ่มของจุดอ่อนตาม [1] สำหรับข้อบกพร่องทางด้านความปลอดภัย และได้ทำการประเมินโดยใช้ข้อมูลของจุดอ่อนที่เกิดขึ้นกับระบบปฏิบัติการรวมทั้งสิ้น 1360 รายการ จากจุดอ่อนที่เกิดบนวินโดวส์เอ็นที 1200 รายการ และจุดอ่อนที่เกิดบนลินุกซ์เรดแฮท 160 รายการ

2.3.3 งานวิจัย “Assessing computer security vulnerability”

Alves-Foss และคณะ [12] ได้เสนอเกณฑ์ในการวัดความเปราะบางสำหรับความปลอดภัยทางด้านคอมพิวเตอร์ ที่เรียกว่า เอสวีไอ (System Vulnerability Index(SVI)) โดยพิจารณาจากปัจจัยที่มีผลกระทบต่อความปลอดภัย เพื่อกำหนดเป็นเกณฑ์มาตรฐานสำหรับชี้ให้เห็นถึงระดับของความเปราะบางที่เกิดขึ้นในระบบคอมพิวเตอร์ ค่าของเอสวีไอจะมีค่าอยู่ระหว่าง 0 ถึง 1 โดยเอสวีไอที่มีค่ามากแสดงว่าระดับของความเปราะบางของระบบมีสูงกว่าเอสวีไอที่มีค่าน้อย

จากทฤษฎีและงานวิจัยที่ได้กล่าวมาในบทที่ 2 นี้ เป็นแนวทางในการจัดกลุ่มของจุดอ่อนและข้อผิดพลาดที่เกิดขึ้นในระบบคอมพิวเตอร์ แนวทางในการคิดคำนวณคะแนนความเปราะบาง รวมถึงแนวทางในการวิเคราะห์และประเมินผลจุดอ่อนและความเปราะบางที่เกิดขึ้น

ซึ่งก่อนทำการจัดกลุ่มของจุดอ่อนจะต้องผ่านขั้นตอนในการคัดเลือกจุดอ่อนที่มีลักษณะตรงกับวัตถุประสงค์ของงานวิจัยนี้ก่อน ได้แก่จุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์ประเภทต่างๆ ซึ่งในบทที่ 3 จะได้กล่าวถึงรายละเอียดของวิธีการคัดเลือกข้อมูลจุดอ่อนและการจัดเก็บข้อมูลที่ได้จากการคัดเลือกต่อไป

บทที่ 3

การคัดเลือกและการจัดเก็บข้อมูลจุดอ่อน

ในบทนี้จะกล่าวถึงวิธีการคัดเลือกจุดอ่อนจากข้อมูลจุดอ่อนที่ปรากฏในรายการซีวีอี อธิบายรายละเอียดโครงสร้างตารางจัดเก็บข้อมูลว่ามีส่วนประกอบอย่างไรบ้าง รวมถึงแสดงตัวอย่างตารางจัดเก็บข้อมูลจุดอ่อนที่ได้ ซึ่งมีรายละเอียดในส่วนต่างๆดังต่อไปนี้

3.1 การคัดเลือกข้อมูลจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์จากรายการซีวีอี

การคัดเลือกจุดอ่อนจากข้อมูลจุดอ่อนในรายการซีวีอีเพื่อใช้ในงานวิจัยนี้ มีอยู่ 2 ขั้นตอน คือ

3.1.1 **คัดเลือกจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์** จะทำการคัดเลือกจุดอ่อนจากรายการจุดอ่อนในซีวีอีทั้งหมด โดยเลือกเอาเฉพาะจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์เท่านั้น และตัดเอาจุดอ่อนส่วนอื่นๆที่ไม่เกี่ยวข้องออกไป เช่น จุดอ่อนที่เกิดขึ้นกับซอร์ฟแวร์ของเครื่องลูกข่าย(Client), จุดอ่อนที่เกิดขึ้นกับระบบปฏิบัติการ, จุดอ่อนที่เกิดขึ้นกับอุปกรณ์(Hardware) เป็นต้น พร้อมทั้งระบุอย่างคร่าวๆในเบื้องต้นว่าจุดอ่อนนั้นเกิดขึ้นบนเซิร์ฟเวอร์ประเภทใด โดยจะพิจารณาจากเนื้อหาในส่วนที่เป็นคำอธิบาย (Description) ที่ระบุไว้ในรายการซีวีอีซึ่งก็พอที่จะทำให้ทราบได้อย่างคร่าวๆว่าจุดอ่อนนั้นๆเกิดขึ้นกับซอร์ฟแวร์หรือโปรแกรมประยุกต์ที่ทำงานบนเซิร์ฟเวอร์หรือไม่ แต่ส่วนใหญ่จะพบว่าเนื้อหาในส่วนคำอธิบายของซีวีอีมีน้อยเกินไปและอธิบายไม่ละเอียดมากนักทำให้ไม่สามารถตัดสินใจได้ว่าจุดอ่อนในรายการนั้นเป็นจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์หรือไม่ จึงจำเป็นที่จะต้องเข้าไปดูรายละเอียดเพิ่มเติมจากที่ระบุไว้ในส่วนแหล่งข้อมูลอ้างอิงของรายการซีวีอีเพิ่มเติม ซึ่งอาจจะเป็นลิงค์ของเว็บไซต์ที่สามารถเข้าดูได้เลย หรืออาจเป็นเพียงข้อมูลอ้างอิงรายการจุดอ่อนที่กำหนดโดยองค์กรต่างๆแต่ละองค์กร ซึ่งบางครั้งอาจต้องค้นหาข้อมูลจากแหล่งข้อมูลอื่นๆเพิ่มเติมด้วย ได้แก่ [7],[8],[9] จากตัวอย่างข้อมูลจุดอ่อนในรายการซีวีอีในตารางที่ 3.1 CVE-1999-0006 สามารถดูรายละเอียดจากคำอธิบายและสรุปได้ว่าจุดอ่อนที่เกิดขึ้นน่าจะเป็นจุดอ่อนที่เกิดขึ้นบนเมล์เซิร์ฟเวอร์ ในขณะที่ CVE-1999-0055 ดูจากคำอธิบายแล้วยังไม่สามารถสรุปได้ชัดเจนว่าเป็นจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์หรือไม่ จึงจำเป็นต้องค้นหาข้อมูลรายละเอียดเพิ่มเติมจากข้อมูลอ้างอิงขององค์กรต่างๆตามที่ระบุไว้ในซีวีอี ซึ่งประกอบไปด้วย SUN:00172, AIXAPAR:IX80543,RSI:RSI.0005.05-14-98.SUN.LIBNSL และ XF:sun-libnsl ซึ่งโครงสร้างของข้อมูลอ้างอิง ประกอบด้วย แหล่งข้อมูล และรหัสอ้างอิง การค้นหาข้อมูลเพิ่มเติมจากแหล่งข้อมูลอ้างอิงในรายการซีวีอีจะต้องนำรหัสอ้างอิงที่ระบุไว้ในรายการซีวีอีนั้นไปค้นหาจากแหล่งข้อมูล

ต่างๆตาม[5] ซึ่งมีรายชื่อดังแสดงในตารางที่ 3.2 และในตารางที่ 3.3 จะแสดงตัวอย่างรายละเอียดของแหล่งข้อมูลจุดอ่อนในตารางที่ 3.2 ซึ่งในรายละเอียดดังกล่าวจะระบุถึงเว็บไซต์ของแหล่งข้อมูลนั้นๆที่สามารถเข้าไปทำการค้นหาข้อมูลเพิ่มเติมได้

Name	Description	References
CVE-1999-0006	Buffer overflow in POP servers based on BSD/Qualcomm's qpopper allows remote attackers to gain root access using a long PASS command.	CERT:CA-98.08.qpopper_vul,SGI:19980801-01-I,AUSCERT:AA-98.01,XF:qpopper-pass-overflow,BID:133
CVE-1999-0055	Buffer overflows in Sun libnsl allow root access.	SUN:00172,AIXAPAR:IX80543,RSI:RSI.0005.05-14-98.SUN.LIBNSL,XF:sun-libnsl

ตารางที่ 3.1 แสดงตัวอย่างข้อมูลจุดอ่อนในรายการซีวีอี ซึ่งประกอบไปด้วยหมายเลขซีวีอี คำอธิบาย และแหล่งข้อมูลอ้างอิง

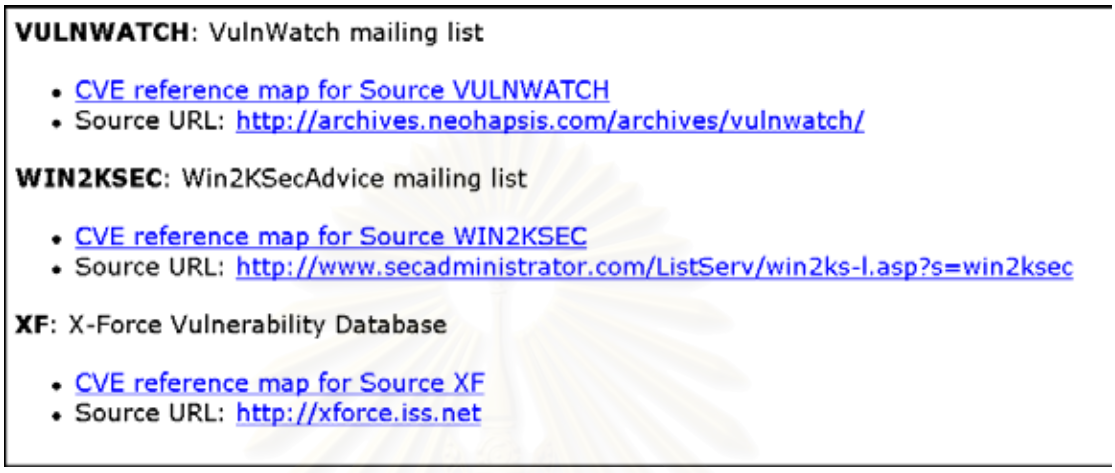
SOURCE LIST				
AIXAPAR	ALLAIRE	APPLE	ASCEND	ATSTAKE
AUSCERT	BID	BINDVIEW	BUGTRAQ	CALDERA
CERT	CERT-VN	CHECKPOINT	CIAC	CISCO
COMPAQ	CONECTIVA	CONFIRM	DEBIAN	EEYE
EL8	ENGARDE	ERS	FEDORA	FREEBSD
FRSIRT	FULLDISC	FarmerVenema	FreeBSD	GENTOO
HERT	HP	IBM	IDEFENSE	IMMUNIX
INFOWAR	ISS	KSRT	LOPHT	MANDRAKE
MANDRIVA	MISC	MLIST	MS	MSKB
NAI	NETBSD	NETECT	NTBUGTRAQ	NetBSD
OPENBSD	OPENPKG	OSVDB	OVAL	REDHAT
RSI	SCO	SECTRACK	SECUNIA	SEKURE
SF-INCIDENTS	SGI	SLACKWARE	SNI	SUN
SUNALERT	SUNBUG	SUSE	TRUSTIX	TURBO
UBUNTU	URL	VULN-DEV	VULNWATCH	WIN2KSEC
XF				

ตารางที่ 3.2 แสดงรายชื่อแหล่งข้อมูลจุดอ่อนต่าง ๆ

SOURCE DETAILS
ALLAIRE: Allaire Security Bulletin • CVE reference map for Source ALLAIRE • Source URL: http://www.macromedia.com/v1/developer/securityzone/ • Notes: Allaire was acquired by Macromedia. ALLAIRE references might be converted into MACROMEDIA references in the future.
APPLE: Apple Security Update • CVE reference map for Source APPLE • Source URL: http://lists.apple.com/archives/security-annouce

ตารางที่ 3.3 แสดงตัวอย่างรายละเอียดของแหล่งข้อมูลจุดอ่อนต่าง ๆ

วิธีการหารายละเอียดข้อมูลเพิ่มเติม จากตัวอย่างข้อมูลอ้างอิงของ CVE-1999-0055 เช่น XF:sun-libnsl XF คือ ชื่อของแหล่งข้อมูลจุดอ่อน และ sun-libnsl คือ รหัสอ้างอิง ในการค้นหาข้อมูลเพิ่มเติมจะต้องดูว่าข้อมูลอ้างอิงนั้นเป็นของแหล่งข้อมูลใด ในที่นี้คือ XF จากนั้น จึงเข้ามาค้นหารายละเอียดของ XF ใน [5] ดังรูป 3.1



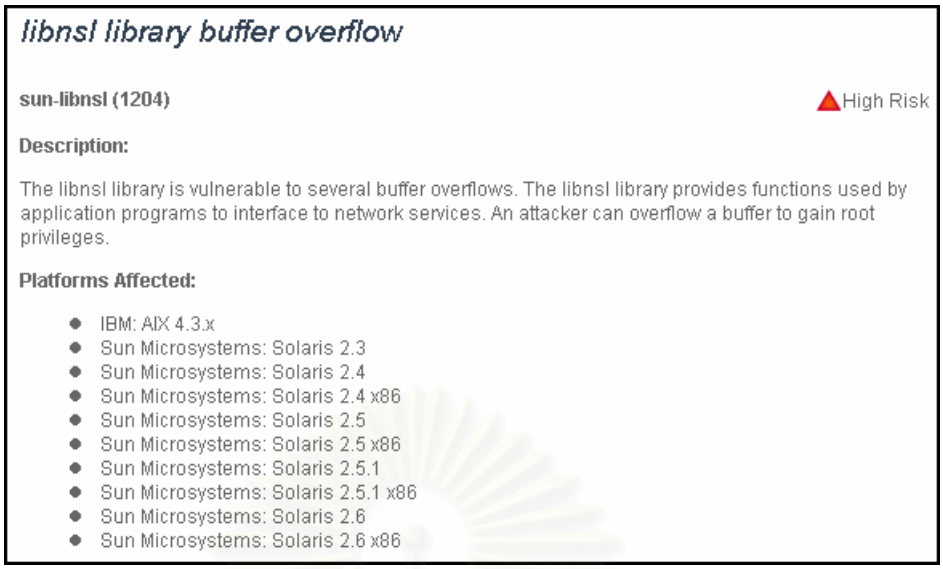
รูปที่ 3.1 แสดงรายละเอียดของแหล่งข้อมูลจุดอ่อน XF

จากนั้นจึงไปที่เว็บไซต์ของ XF (X-Force Vulnerability Database) เพื่อค้นหารายละเอียดของจุดอ่อนจากรหัสอ้างอิง ซึ่งในที่นี้ คือ sun-libnsl ต่อไป ดังรูปที่ 3.2 – 3.5

รูปที่ 3.2 เว็บไซต์ของ X-Force Vulnerability Database

รูปที่ 3.3 แสดงผลตัวอย่างการหาข้อมูลของรหัสอ้างอิง sun-libnsl

รูปที่ 3.4 ตัวอย่างรายละเอียดข้อมูลจุดอ่อนที่ได้จากการค้นหารหัสอ้างอิง sun-libnsl



libnsl library buffer overflow

sun-libnsl (1204) High Risk

Description:

The libnsl library is vulnerable to several buffer overflows. The libnsl library provides functions used by application programs to interface to network services. An attacker can overflow a buffer to gain root privileges.

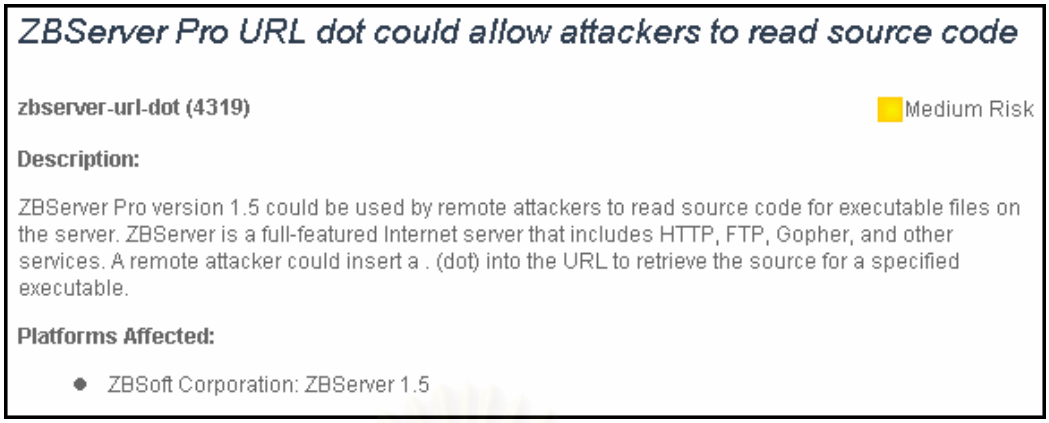
Platforms Affected:

- IBM: AIX 4.3.x
- Sun Microsystems: Solaris 2.3
- Sun Microsystems: Solaris 2.4
- Sun Microsystems: Solaris 2.4 x86
- Sun Microsystems: Solaris 2.5
- Sun Microsystems: Solaris 2.5 x86
- Sun Microsystems: Solaris 2.5.1
- Sun Microsystems: Solaris 2.5.1 x86
- Sun Microsystems: Solaris 2.6
- Sun Microsystems: Solaris 2.6 x86

รูปที่ 3.5 **ภาพขยายของรูปที่** 3.4 **ตัวอย่างรายละเอียดข้อมูลจุดอ่อนที่ได้จากการค้นหารหัสอ้างอิง** sun-libnsl

จากรูปที่ 3.5 เมื่ออ่านจากรายละเอียดที่ได้ทำให้สามารถสรุปได้ว่า CVE-1999-0055 ไม่ถือว่าเป็นจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์

3.1.2 **คัดแยกข้อมูลจุดอ่อนที่ได้จาก** 3.1.1 **ออกตามประเภทของเซิร์ฟเวอร์** ในขั้นตอนนี้จะทำการคัดแยกรายการจุดอ่อนที่ได้ในขั้นตอนที่ 1 ออกตามชนิดของเซิร์ฟเวอร์ต่างๆซึ่งแบ่งออกได้ทั้งหมด 29 เซิร์ฟเวอร์ตามที่ระบุไว้ในบทที่ 1 ข้อที่ 1.3 การระบุว่าจุดอ่อนรายการนั้นเป็นจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์ใดจะพิจารณาว่าจุดอ่อนจุดนั้นมีผลกระทบกับเซิร์ฟเวอร์อะไรบ้าง รวมถึงเก็บรายละเอียดต่างๆที่จำเป็นต้องใช้ในการจัดกลุ่มจุดอ่อน และข้อมูลของระบบปฏิบัติการที่ได้รับผลกระทบจากจุดอ่อนนั้นๆ โดยพิจารณาจากคำอธิบายที่ระบุในซีวีอี และรายละเอียดเพิ่มเติมที่ได้จากแหล่งข้อมูลอ้างอิง ซึ่งวิธีการหารายละเอียดเพิ่มเติมนั้นได้กล่าวไว้แล้วในข้อ 3.1.1 ในกรณีที่จุดอ่อนจุดนั้นเกิดขึ้นกับซอฟต์แวร์เซิร์ฟเวอร์ที่ทำหน้าที่ให้บริการมากกว่า 1 บริการ ก็จะถือว่าจุดอ่อนรายการนั้นเป็นจุดอ่อนที่เกิดบนเซิร์ฟเวอร์มากกว่า 1 ชนิดเช่นกัน เช่น CVE-2000-0004 ในตัวอย่างรูป 3.6



ZBServer Pro URL dot could allow attackers to read source code

zbserver-url-dot (4319) Medium Risk

Description:

ZBServer Pro version 1.5 could be used by remote attackers to read source code for executable files on the server. ZBServer is a full-featured Internet server that includes HTTP, FTP, Gopher, and other services. A remote attacker could insert a . (dot) into the URL to retrieve the source for a specified executable.

Platforms Affected:

- ZBSoft Corporation: ZBServer 1.5

รูปที่ 3.6 ตัวอย่างรายละเอียดข้อมูลจุดอ่อนของ CVE-2000-0004 ที่ค้นหาได้จากแหล่งข้อมูล XF

จากคำอธิบายที่ปรากฏในรูป 3.8 ZBServer Pro ทำหน้าที่ให้บริการเกี่ยวกับเว็บ, เอฟทีพี และโกเฟอร์ ดังนั้นจึงถือว่า CVE-2000-0004 เป็นจุดอ่อนที่สามารถเกิดขึ้นได้กับเซิร์ฟเวอร์ทั้งหมด 3 เซิร์ฟเวอร์ ได้แก่ เว็บเซิร์ฟเวอร์, เอฟทีพีเซิร์ฟเวอร์ และโกเฟอร์เซิร์ฟเวอร์ นั่นเอง ซึ่งเซิร์ฟเวอร์บางประเภทอาจมีการแบ่งย่อยลงไปอีก เช่น ดาต้าเบสเซิร์ฟเวอร์ สามารถแบ่งออกได้เป็น Microsoft SQL , Oracle ฯลฯ ทั้งนี้ขึ้นอยู่กับข้อมูลรายละเอียดที่รวบรวมได้ในการค้นหาข้อมูลจากแหล่งข้อมูลต่างๆ

3.2 การจัดกลุ่มจุดอ่อน

งานวิจัยนี้อาศัยหลักเกณฑ์การจัดกลุ่มจุดอ่อนตามงานวิจัยของรัศมีทิพย์ วิตา[3] ซึ่งเป็นงานที่เสริมวิธีการจัดกลุ่มของ Landwehr [1] โดยทำการแบ่งจุดอ่อนออกเป็น 4 รูปแบบด้วยกัน ได้แก่

1. ประเภทของจุดอ่อน
2. จุดที่เกิดจุดอ่อน
3. ลักษณะความเสียหาย
4. ระดับความรุนแรง

3.2.1 ประเภทของจุดอ่อน การจัดกลุ่มจุดอ่อนประเภทนี้ จะจัดกลุ่มออกตามลักษณะของความผิดพลาดที่เกิดขึ้นในระบบ ซึ่งแบ่งออกได้เป็น 9 ประเภทด้วยกัน ได้แก่

1. ความผิดพลาดของการตรวจสอบข้อมูลนำเข้า (Input Validation Error)

2. ความผิดพลาดของขอบเขตข้อมูล (Boundary Overflow)

3. ความผิดพลาดในการตรวจสอบการเข้าถึง (Access Validation Error)

4. ความผิดพลาดของการเหลื่อมล้ำของการตรวจสอบสิทธิ (Serialization)

5. ความผิดพลาดของการปรับแต่งระบบ (Configuration Error)

6. ความผิดพลาดจากสภาพแวดล้อม (Environmental Error)

7. ความผิดพลาดจากการออกแบบระบบ (Design Error)

8. ความผิดพลาดจากชุดคำสั่งจัดการข้อยกเว้น (Exceptional Condition Handling Error)

9. อื่นๆ (Others)

3.2.2 **จุดที่เกิดจุดอ่อน** การจัดกลุ่มจุดอ่อนประเภทนี้ จะจัดกลุ่มตามตำแหน่งของจุดอ่อนหรือความผิดพลาดที่เกิดขึ้นในระบบ ซึ่งแบ่งออกได้เป็น 8 ตำแหน่งด้วยกัน ได้แก่

1. ส่วนการเริ่มต้นระบบ (System Initiation)

2. ส่วนการจัดการหน่วยความจำ (Memory Management)

3. ส่วนการจัดการการประมวลผล (Process Management)

4. ส่วนการจัดการอุปกรณ์ (Device Management)

5. ส่วนการจัดการแฟ้มข้อมูล (File Management)

6. ส่วนการพิสูจน์ตัวจริง (Authentication)

7. ส่วนโปรแกรมที่สนับสนุนการทำงานของระบบปฏิบัติการ (Support)

8. ส่วนโปรแกรมประยุกต์ (Application)

3.2.3 **ลักษณะความเสียหาย** การจัดกลุ่มจุดอ่อนประเภทนี้ จะจัดกลุ่มตามลักษณะความเสียหายที่เกิดขึ้น อันจะนำไปสู่การเสียความเป็นความลับ การเสียบูรณะภาพ การเสียสภาพพร้อมใช้งาน และการล่วงละเมิดระบบ ซึ่งความเสียหายต่างๆที่เกิดขึ้นมีรายละเอียดดังต่อไปนี้

1. เสียความเป็นความลับ (Confidentiality)

2. เสียสภาพบูรณภาพ (Integrity)

3. เสียสภาพพร้อมใช้งาน (Availability)

4. ระบบถูกล่วงละเมิด (System Compromise) เป็นความเสียหายจากจุดอ่อน ซึ่งผลจากการโจมตีจะส่งผลให้ผู้โจมตีได้รับเอกสิทธิ์ในการเข้าใช้งานระบบ โดยการล่วงละเมิดระบบแบ่งย่อยความเสียหายที่เกิดขึ้นออกได้เป็น 4 ลักษณะ ดังต่อไปนี้

- เรียกทำงานชุดคำสั่งใดๆ (Run Arbitrary Code)

- เพิ่มสิทธิการใช้งาน (Elevate Privilege)

- เข้าถึงบัญชีผู้ใช้ (Account Break-in)

- เข้าถึงระดับราก (Root Break-in)

3.2.4 **ระดับความรุนแรง** การจัดกลุ่มจุดอ่อนประเภทนี้ จะจัดกลุ่มตามความเสียหายที่เกิดขึ้น เนื่องจากจุดอ่อนแต่ละรายการสามารถก่อให้เกิดความเสียหายมากน้อย ไม่เท่ากัน จึงจำเป็นต้องแบ่งระดับความรุนแรงของความเสียหายที่เกิดขึ้นนั้น โดยจะแบ่งระดับความความรุนแรงที่เกิดขึ้นออกเป็น 3 ระดับด้วยกัน ได้แก่

1. ระดับสูง (High)

2. ระดับกลาง (Medium)

3. ระดับต่ำ (Low)

3.3 โครงสร้างตารางจัดเก็บข้อมูล

ตารางที่ใช้ในการจัดเก็บข้อมูลสำหรับงานวิจัยนี้ในเบื้องต้นจะจัดเก็บอยู่ในรูปแบบของแฟ้มข้อมูลเอ็กซ์เซล (Excel) โดยแยกแต่ละแฟ้มข้อมูลออกตามชนิดของเซิร์ฟเวอร์ ซึ่งจะได้ทั้งหมด 29 แฟ้มข้อมูล ตารางดังกล่าวแบ่งออกได้ถึงหมด 2 ส่วนด้วยกัน คือ ส่วนหัวข้อเรื่อง และส่วนรายละเอียด โดยส่วนหัวข้อเรื่องจะประกอบไปด้วย 6 ส่วนย่อยๆ ได้แก่

1. รายการซีวีอี ประกอบไปด้วย ชื่อซีวีอี(Name), คำอธิบาย(Description) และแหล่งข้อมูลอ้างอิง(References) (รูปที่ 3.7)

2. กลุ่มของจุดอ่อน ซึ่งแบ่งออกเป็น 4 รูปแบบ ดังที่กล่าวไว้แล้วในหัวข้อ 3.2 (รูปที่ 3.7)

3. ขอบเขตการโจมตี แบ่งเป็น การโจมตีจากระยะใกล้ (Local) และโจมตีจากระยะไกล (Remote) (รูปที่ 3.7)

4. ซอร์ฟแวร์ที่เกิดจุดอ่อน ประกอบด้วย ชื่อซอร์ฟแวร์ และเวอร์ชันที่เกิดจุดอ่อน (รูปที่ 3.7)

5.ประเภทของเซิร์ฟเวอร์ ทั้งหมด 29 เซิร์ฟเวอร์ ซึ่งบางเซิร์ฟเวอร์อาจจะมีการแบ่งประเภทย่อยลงไปอีก ทั้งนี้หลักเกณฑ์การแบ่งประเภทย่อยของเซิร์ฟเวอร์ จะพิจารณาจากข้อมูลรายละเอียดจุดอ่อนที่รวบรวมได้ในขั้นตอนที่ 3.1.2 โดยการแบ่งประเภทย่อยของเซิร์ฟเวอร์ก็เพื่อต้องการเก็บรายละเอียดของเซิร์ฟเวอร์นั้นๆให้ได้มากที่สุด ซึ่งอาจเป็นประโยชน์ในการนำข้อมูลที่ได้ไปใช้ในการวิเคราะห์ต่อไปในภายหลัง (รูปที่ 3.7 – 3.8)

6. ระบบปฏิบัติการที่ได้รับผลกระทบจากจุดอ่อน (รูปที่ 3.9 – 3.11) ประกอบไปด้วย ระบบปฏิบัติการยูนิกซ์, ลินุกซ์, วินโดวส์, โอเอสทู, เน็ตแวร์, ซิสโก้ไอโอเอส, แคชโอเอส และระบบปฏิบัติการที่ไม่ได้มีการระบุไว้ ซึ่งเป็นกลุ่มที่จัดไว้สำหรับจุดอ่อนที่ไม่ได้มีรายละเอียดบอกว่าจุดอ่อนนั้นมีผลกระทบกับระบบปฏิบัติการใดบ้างถึงแม้ว่าจะค้นหารายละเอียดจากแหล่งข้อมูลอ้างอิงแล้วก็ตาม ทั้งนี้หลักเกณฑ์การแบ่งประเภทของระบบปฏิบัติการ จะพิจารณาจากข้อมูลรายละเอียดจุดอ่อนที่รวบรวมได้ในขั้นตอนที่ 3.1.2 เช่นเดียวกัน ซึ่งจากการรวบรวมข้อมูลรายละเอียดจากแหล่งอ้างอิง พบว่าข้อมูลรายละเอียดของจุดอ่อนที่ระบุถึงระบบปฏิบัติการที่ได้รับผลกระทบจากจุดอ่อนนั้น แบ่งออกได้เป็น 3 ลักษณะ ดังนี้

1. มีการระบุชื่อพร้อมทั้งเวอร์ชันของระบบปฏิบัติการที่ได้รับผลกระทบอย่างละเอียดชัดเจน

2. มีการระบุชื่อของระบบปฏิบัติการที่ได้รับผลกระทบแต่ไม่ได้ระบุเวอร์ชันที่ได้รับผลกระทบไว้

3. ไม่มีการระบุรายละเอียดของระบบปฏิบัติการที่ได้รับผลกระทบเลย

ดังนั้นในการเก็บรายละเอียดของระบบปฏิบัติการที่ได้รับผลกระทบในงานวิจัยนี้จึงได้กำหนดรูปแบบการจัดเก็บข้อมูลของระบบปฏิบัติการแต่ละประเภท ดังตารางที่ 3.4

OS		
Specified	Not Specified	Version

ตารางที่ 3.4 รูปแบบตารางการเก็บข้อมูลของระบบปฏิบัติการ

จากตารางที่ 3.4 แสดงรูปแบบตารางเก็บข้อมูลของระบบปฏิบัติการที่ได้รับผลกระทบจากจุดอ่อน โดยประกอบด้วยส่วนต่างๆดังต่อไปนี้

1. OS คือ ชื่อระบบปฏิบัติการที่ได้รับผลกระทบ
2. Specified คือ เขตข้อมูลที่ใช้เพื่อระบุว่าข้อมูลรายละเอียดจากแหล่งอ้างอิงที่ได้มีการระบุเวอร์ชันของระบบปฏิบัติการที่ได้รับผลกระทบนี้หรือไม่ ถ้ามีจึงกำหนดเครื่องหมาย “/” ลงในเขตข้อมูลนี้ พร้อมทั้งทำการระบุเวอร์ชันที่ได้รับผลกระทบลงในเขตข้อมูลเวอร์ชัน
3. Not Specified ในกรณีที่ข้อมูลรายละเอียดจากแหล่งอ้างอิงที่ได้ ระบุแต่ชื่อของระบบปฏิบัติการ แต่ไม่ได้ระบุว่ามีผลกระทบกับระบบปฏิบัติการเวอร์ชันอะไร ให้ทำเครื่องหมาย “/” ลงในเขตข้อมูลนี้
4. Version คือ เขตข้อมูลที่ใช้เก็บชื่อเวอร์ชันของระบบปฏิบัติการที่ได้รับผลกระทบจากจุดอ่อน

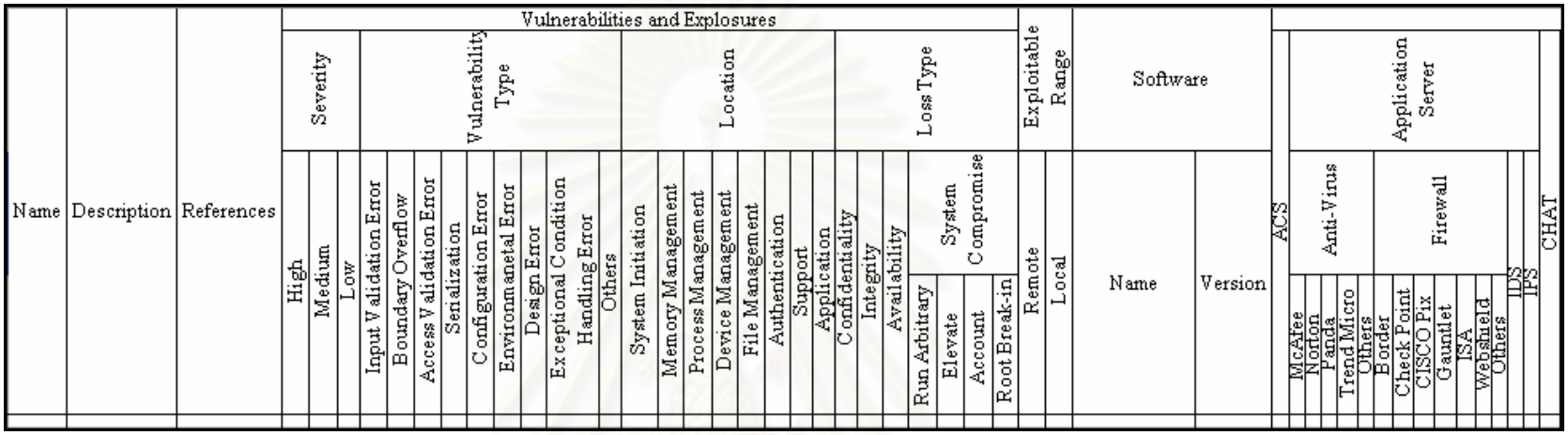
ในกรณีที่ระบบปฏิบัติการเป็น วินโดวส์เอ็กซ์พี จะเก็บข้อมูลโดยแบ่งเป็น “Home” สำหรับ Windows XP(Home Edition) และ “Pro” สำหรับ Windows XP(Professional)

สำหรับระบบปฏิบัติการยูนิกซ์ ลินุกซ์และวินโดวส์ ในเขตข้อมูล Not Specified(Unix), Not Specified(Linux) และ Not Specified(Windows) จะทำเครื่องหมาย “/” ลงในเขตข้อมูลเหล่านี้เมื่อข้อมูลรายละเอียดเพิ่มเติมจากแหล่งอ้างอิงของข้อมูลจุดอ่อนนั้นๆ ระบุเพียงว่าจุดอ่อนจุดนั้นๆ มีผลกระทบกับระบบปฏิบัติการยูนิกซ์ ลินุกซ์ หรือวินโดวส์ โดยไม่ได้มีการระบุแพลตฟอร์มและเวอร์ชันที่ได้รับผลกระทบของแต่ละระบบปฏิบัติการ ส่วนเขตข้อมูล Not Specified ในช่อง

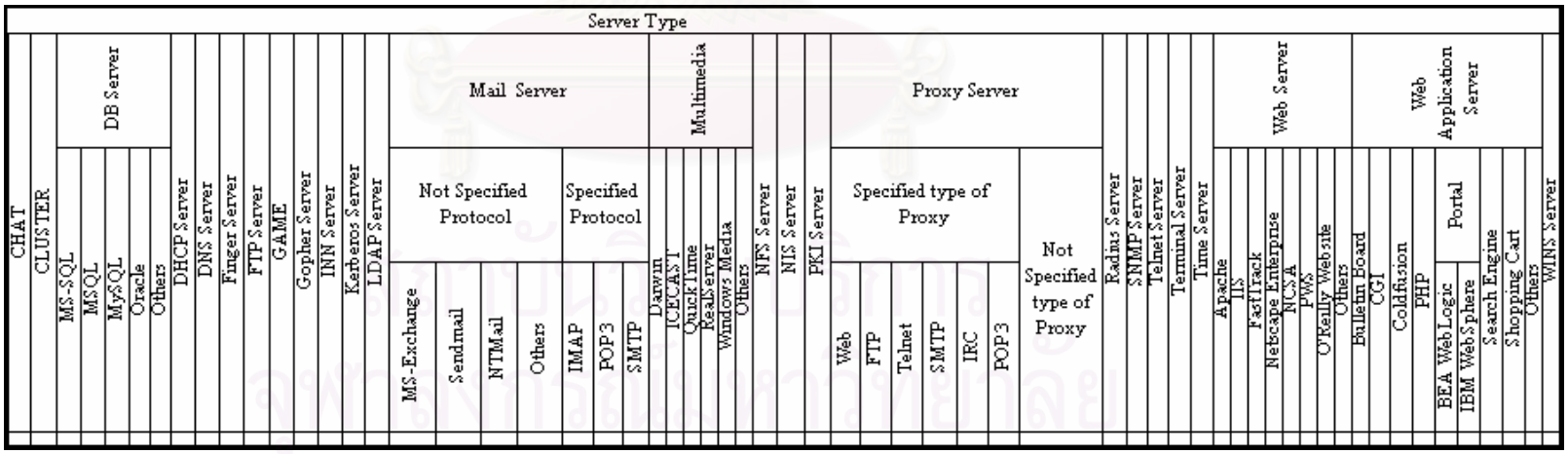
ท้ายสุดของตารางจัดเก็บข้อมูลจุดอ่อน จะกำหนดเครื่องหมาย “/” ลงในเขตข้อมูลนี้ เฉพาะในกรณีที่ข้อมูลรายละเอียดจากแหล่งอ้างอิงไม่มีการระบุไว้เลยว่าจุดอ่อนที่เกิดขึ้นนั้นส่งผลกระทบต่อระบบปฏิบัติการใด

ในส่วนที่ 2 ของโครงสร้างตารางจัดเก็บข้อมูลเป็นส่วนของรายละเอียด จะเก็บรายละเอียดต่างๆตามที่ได้แบ่งไว้ในส่วนของหัวข้อเรื่องดังที่กล่าวมาแล้วข้างต้น โดยตัวอย่างการจัดเก็บข้อมูลลงในตารางจัดเก็บข้อมูลสามารถดูได้ในข้อ 3.4

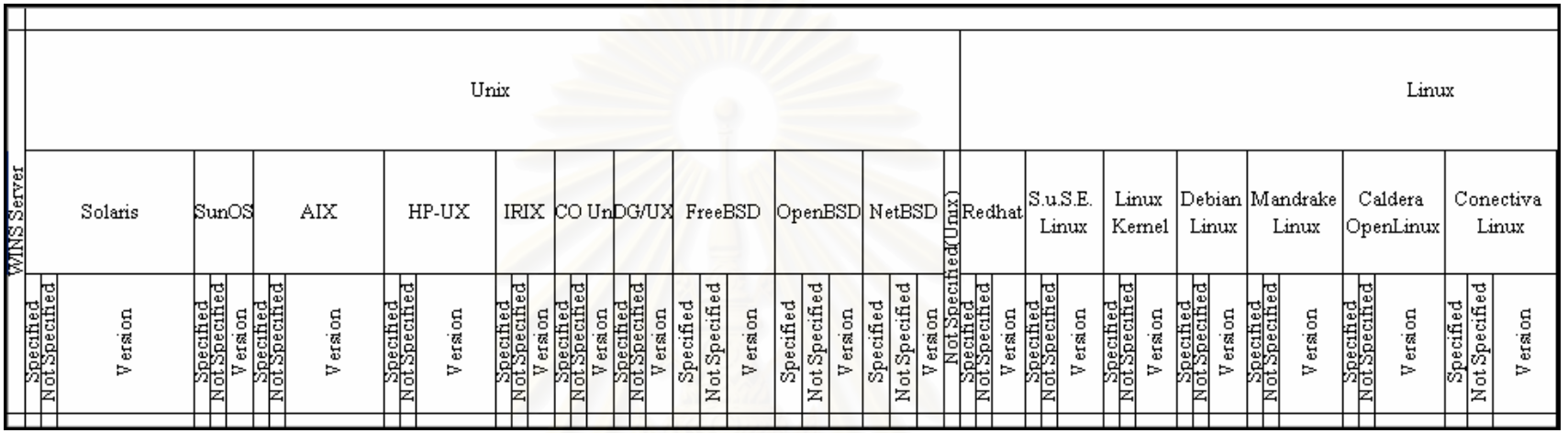
ในรูปที่ 3.7 – 3.11 แสดงแม่แบบตารางที่ใช้ในการจัดเก็บข้อมูลสำหรับงานวิจัยนี้ โดยตารางที่เห็นทั้งหมดในรูปที่ 3.7 – 3.11 นี้ ความจริงแล้วไม่ได้แยกออกเป็น 5 ตาราง แต่เรียงต่อกันยาวเป็นตารางเดียว



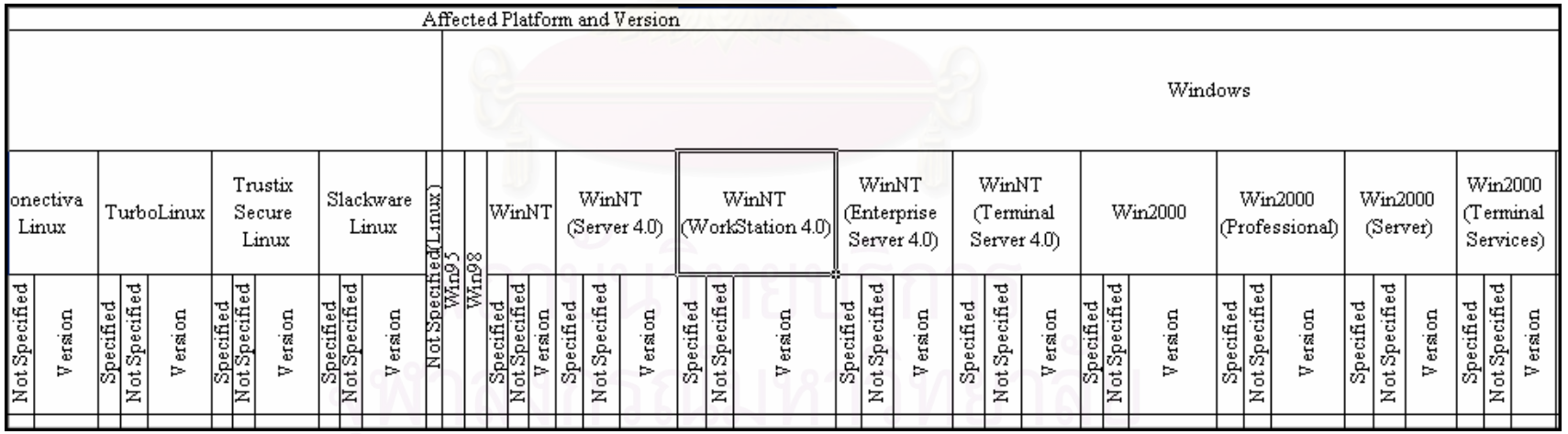
รูปที่ 3.7 **แสดงแม่แบบตารางการจัดเก็บข้อมูลจุดอ่อน#1**



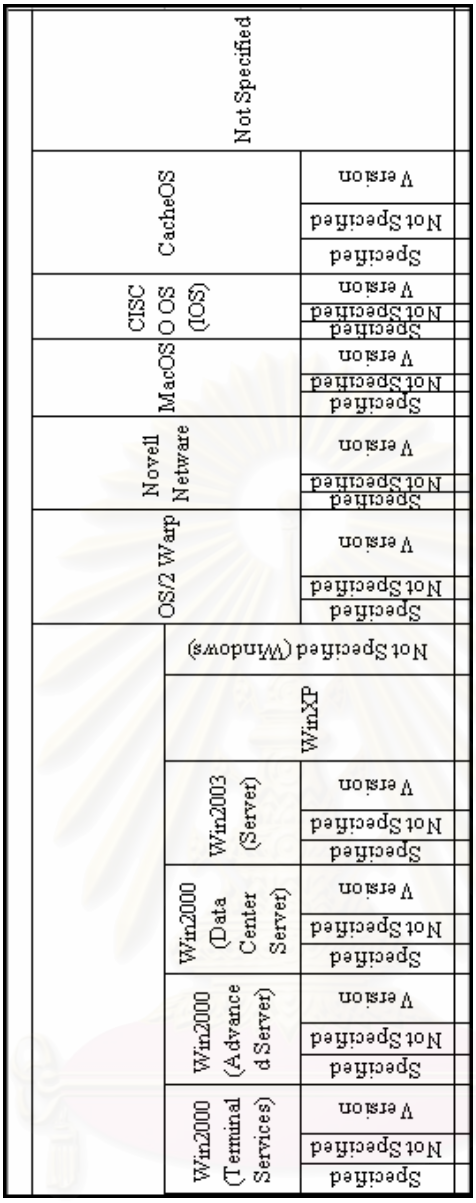
รูปที่ 3.8 **แสดงแม่แบบตารางการจัดเก็บข้อมูลจุดอ่อน#2**



รูปที่ 3.9 **แสดงแม่แบบตารางการจัดเก็บข้อมูลจุดอ่อน#3**



รูปที่ 3.10 **แสดงแม่แบบตารางการจัดเก็บข้อมูลจุดอ่อน#**4



รูปที่ 3.11 แสดงแม่แบบตารางการจัดเก็บข้อมูลจุดอ่อน#5

จากแม่แบบตารางที่ได้ ในขั้นตอนการจัดเก็บข้อมูลเพื่อลดความผิดพลาดที่อาจเกิดขึ้นได้ จึงได้แยกการจัดเก็บข้อมูลออกเป็นตารางย่อยเพื่อจัดเก็บเฉพาะข้อมูลจุดอ่อนที่เกิดขึ้นบนแต่ละเซิร์ฟเวอร์เท่านั้น

3.4 ตัวอย่างบางส่วนของตารางการจัดเก็บข้อมูล

หลังจากที่คัดแยกจุดอ่อนที่เกิดขึ้นออกตามประเภทของเซิร์ฟเวอร์และรวบรวมรายละเอียดต่างๆเกี่ยวกับจุดอ่อนแล้ว จึงนำข้อมูลที่ได้จัดเก็บลงในตารางจัดเก็บข้อมูลของแต่ละเซิร์ฟเวอร์นั้นๆ ดังเช่นตัวอย่างในตารางที่ 3.5 เป็นตัวอย่างบางส่วนของตารางแสดงการจัดเก็บข้อมูลจุดอ่อนที่เกิดขึ้นบน Database Server เนื่องจากตารางการจัดเก็บข้อมูลนี้มีขนาดยาวมาก ประกอบไปด้วยเขตข้อมูลสำหรับมุมมองทุกๆมิติของแต่ละรายการซีวีอี ตัวอย่างเหล่านี้จึงตัดเขต

ข้อมูลบางส่วนที่ไม่เกี่ยวข้องออก ซึ่งได้แก่เขตข้อมูลที่เกี่ยวข้องกับประเภทของเซิร์ฟเวอร์ จะสังเกตได้ว่าเขตข้อมูลต่างๆเหล่านี้จะ Mutually Excusive กันเป็นส่วนมาก เพราะเมื่อเป็นของเซิร์ฟเวอร์ประเภทหนึ่งไปแล้ว จะไม่เป็นเซิร์ฟเวอร์ประเภทที่เหลือ แต่ซีวีอีรายการหนึ่งอาจจะมีผลต่อหลายๆเซิร์ฟเวอร์หรือมีผลต่อมุมมองในหลายๆมิติได้เช่นกัน

จากหลักเกณฑ์การคัดเลือกข้อมูลจุดอ่อน การรวบรวมข้อมูลจุดอ่อนต่างๆ ทำการจัดกลุ่มของจุดอ่อน และจัดเก็บข้อมูลจุดอ่อนที่ได้ หลังจากเสร็จสิ้นกระบวนการต่างๆในขั้นตอนเหล่านี้แล้ว ในบทต่อไป จะเป็นการคำนวณปริมาณจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์และการคำนวณคะแนนความเปราะบางต่อการโจมตีที่มีอยู่ของเซิร์ฟเวอร์ประเภทต่างๆ

Name	Description	References	Severity: High	Severity: Medium	Severity: Low	Vulnerability Type: Input Validation Error	Boundary Overflow	Access Validation Error	Serialization	Configuration Error	Environmanetal Error	Design Error	Exceptional Condition Handling Error	Others	Location: System Initiation	Memory Management	Process Management	Device Management	File Management	Authentication	Support	Application	Loss Type: Confidentiality	Integrity	Availability	System Compromise: Run Arbitrary	Elevate Privilege	Account Break-in	Root Break-in	Exploitable Range: Remote	Local
CVE-2001-0344	An SQL query method in Microsoft SQL Server 2000 Gold and 7.0 using Mixed Mode allows local database users to gain privileges by reusing a cached connection of the sa administrator account.	MS:MS01-032,CIAC:L-095,XF:mssql-cached-connection-access(6684),OVAL:OVAL71	/									/									/								/		/
CVE-2001-0407	Directory traversal vulnerability in MySQL before 3.23.36 allows local users to modify arbitrary files and gain privileges by creating a database whose name starts with .. (dot dot).	BUGTRAQ:20010318 potential vulnerability of mysqld running with root privileges (can be used as good DoS or r00t expoloit),BUGTRAQ:20010327 MySQL 3.23.36 is relased (fwd),XF:mysql-dot-directory-traversal(6617),BID:2522		/		/							/						/					/			/				/

Name	Software: Name	Software: Version	DB Server: MS-SQL	MSQL	MySQL	Oracle	Others
CVE-2001-0344	Microsoft SQL Server	2000 Gold and 7.0	/				
CVE-2001-0407	MySQL	before 3.23.36			/		

Name	Unix: Solaris Specified	Solaris Not Specified	Solaris Version	SunOS Specified	SunOS Not Specified	SunOS Version	AIX Specified	AIX Not Specified	AIX Version	HP-UX Specified	HP-UX Not Specified	HP-UX Version	IRIX Specified	IRIX Not Specified	IRIX Version	SCO Unix Specified	SCO Unix Not Specified	SCO Unix Version	DG/UX Specified	DG/UX Not Specified	DG/UX Version	FreeBSD Specified	FreeBSD Not Specified	FreeBSD Version	OpenBSD Specified	OpenBSD Not Specified	OpenBSD Version	NetBSD Specified	NetBSD Not Specified	NetBSD Version	Not Specified(Unix)	Red Specified	Red Not Specified
CVE-2001-0344																																	
CVE-2001-0407	/		2.6,7.0,8.0				/		4.3.2,4.3.3	/		11.0,11.11										/		3.5.1,4.2	/		2.6,2.7,2.8					/	

ตารางที่ 3.5 แสดงตัวอย่างบางส่วนของตารางการจัดเก็บข้อมูลจุดอ่อนที่เกิดขึ้นบน Database Server#1

Vulnerabilities and Explosures

Affected Platform and Version																																																																																		
Linux																													Windows																																										OS/2 Warp			Novell Netware			MacOS			CISCO OS (IOS)			Not Specified
lhat	S.u.S.E. Linux			Linux Kernel			Debian Linux			Mandrake Linux			Caldera Open Linux			Conectiva Linux			Turbo Linux			Trustix Secure Linux			Slackware Linux			Not Specified(Linux)	Win95	Win98	WinNT			WinNT (Server 4.0)			WinNT (Work Station 4.0)			WinNT (Enterprise Server 4.0)			WinNT (Terminal Server 4.0)			Win2000			Win2000 (Professional)			Win2000 (Server)			Win2000 (Terminal Services)			Win2000 (Advanced Server)			Win2000 (Data Center Server)			Win2003 (Server)			Win XP	Not Specified (Windows)													
Version	Specified	Not Specified	Version	Specified	Not Specified	Version	Specified	Not Specified	Version	Specified	Not Specified	Version	Specified	Not Specified	Version	Specified	Not Specified	Version	Specified	Not Specified	Version	Specified	Not Specified	Version	Specified	Not Specified	Version				Specified	Not Specified	Version	Specified	Not Specified	Version	Specified	Not Specified	Version	Specified	Not Specified	Version	Specified	Not Specified	Version	Specified	Not Specified	Version	Specified	Not Specified	Version	Specified	Not Specified	Version	Specified	Not Specified	Version	Specified	Not Specified	Version	Specified	Not Specified	Version	Specified	Not Specified	Version			Specified	Not Specified	Version	Specified	Not Specified	Version	Specified	Not Specified	Version	Specified	Not Specified	Version	
																															/		4.0,4.0SP1,4.0SP2,4.0SP3,4.0SP4,4.0SP5,4.0SP6,4.0SP6a																/		SP1, SP2																														
5.2,6.2,7.0	/		6.4,7.0,7.1				/		2.2	/		7.0, 7.1, 7.2																																																																						

ตารางที่ 3.5 แสดงตัวอย่างบางส่วนของตารางการจัดเก็บข้อมูลจุดอ่อนที่เกิดขึ้นบน Database Server#2

บทที่ 4

การนับจำนวนและคำนวณคะแนนความเปราะบางจากข้อมูลจุดอ่อน

จากบทที่ 3 ที่ผ่านมา ทำให้ได้ข้อมูลจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์แต่ละชนิดพร้อมทั้งรายละเอียดต่างๆที่จำเป็นในการวิเคราะห์จุดอ่อนนั้นๆ ในบทนี้จะนำข้อมูลจุดอ่อนที่ได้ทั้งหมดดังกล่าวมาทำการให้คะแนน เพื่อให้สามารถนำผลคะแนนที่ได้ไปใช้ในการวิเคราะห์ความเปราะบางที่มีอยู่บนเซิร์ฟเวอร์ต่างๆต่อไป

4.1 การนับจำนวนจุดอ่อน

การนับจำนวนจุดอ่อนจะนับโดยยึดตามชื่อซีวีอีเป็นหลัก โดย 1 รายการซีวีอี เท่ากับ 1 จุดอ่อน กรณีที่ซีวีอีรายการใดเกิดผลกระทบต่อเซิร์ฟเวอร์มากกว่า 1 เซิร์ฟเวอร์ หากนับจำนวนจุดอ่อนโดยแยกคิดจำนวนจุดอ่อนของแต่ละเซิร์ฟเวอร์จะถือว่า จุดอ่อนรายการนั้นเป็นรายการจุดอ่อนของแต่ละเซิร์ฟเวอร์ไม่เกี่ยวข้องกัน แต่หากทำการนับจำนวนจุดอ่อนของเซิร์ฟเวอร์ทั้งหมดโดยไม่มีการแยกประเภทของเซิร์ฟเวอร์จะถือว่ามีรายการจุดอ่อนเพียง 1 จุดเท่านั้น เช่น CVE-2000-0004 ที่เป็นจุดอ่อนที่เกิดได้บนเซิร์ฟเวอร์ 3 ประเภทด้วยกันได้ แก่ เว็บเซิร์ฟเวอร์, เอฟทีพีเซิร์ฟเวอร์ และโกเฟอร์เซิร์ฟเวอร์ มีรายละเอียดจุดอ่อนคร่าวๆดังนี้

CVE Name : CVE-2000-0004

Description : ZBServer Pro allows remote attackers to read source code for executable files by inserting a . (dot) into the URL.

Severity : Low

Vulnerability Type : Input Validation Error

หากนับจำนวนจุดอ่อนตามระดับความรุนแรงและประเภทของจุดอ่อนโดยแยกประเภทของเซิร์ฟเวอร์ จะถือว่า เว็บเซิร์ฟเวอร์, เอฟทีพีเซิร์ฟเวอร์ และโกเฟอร์เซิร์ฟเวอร์ จะมีจำนวนจุดอ่อนโดยนับตามระดับความรุนแรงเท่ากัน คือ 1 และ จำนวนจุดอ่อนโดยนับตามประเภทของจุดอ่อน คือ 1 เช่นเดียวกัน แต่หากนับจำนวนจุดอ่อนของเซิร์ฟเวอร์ทั้งหมดโดยไม่แยกประเภทของเซิร์ฟเวอร์ ซึ่งจะนับจำนวนจุดอ่อนตามชื่อซีวีอีเป็นหลักแล้ว จะไม่ถือว่าจำนวนจุดอ่อนโดยนับตามระดับความรุนแรงและจำนวนจุดอ่อนโดยนับตามประเภทของจุดอ่อนมีจำนวนอย่างละ 3 จุดอ่อน แต่จะถือว่าเป็นจุดอ่อนที่เกิดจากซีวีอีรายการเดียวกัน ดังนั้น จำนวนจุดอ่อนโดยนับ

ตามระดับความรุนแรงและจำนวนจุดอ่อนโดยนับตามประเภทของจุดอ่อนของเซิร์ฟเวอร์ทั้งหมด โดยไม่มีการแยกประเภท จะมีจำนวนอย่างละ 1 จุดอ่อน เท่านั้น

4.2 การคำนวณคะแนนความเปราะบางจากจุดอ่อน

การให้คะแนนแก่จุดอ่อนจะให้คะแนนตามลักษณะความเสียหายที่เกิดขึ้น ร่วมกับระดับความรุนแรงของจุดอ่อนนั้น แล้วคำนวณผลรวมความเสียหายแต่ละประเภทที่เกิดขึ้น โดยใช้สมการคำนวณตาม [2] โดยมีสมการดังนี้

$$W_i = W_{C_i} + W_{I_i} + W_{A_i}$$

โดยที่ W_i คือ ระดับผลกระทบของจุดบกพร่องใดๆ

W_{C_i} คือ ระดับผลกระทบของจุดบกพร่องใดๆ ที่ส่งผลต่อการรักษาความลับ

W_{I_i} คือ ระดับผลกระทบของจุดบกพร่องใดๆ ที่ส่งผลต่อการบูรณภาพ

W_{A_i} คือ ระดับผลกระทบของจุดบกพร่องใดๆ ที่ส่งผลต่อสภาพพร้อมใช้งาน

i คือ ลำดับของซีวีอี

แต่เนื่องจากในงานวิจัยนี้มีการจัดกลุ่มความเสียหายในลักษณะที่ระบบถูกล่วงละเมิดด้วย ดังนั้นจึงจำเป็นต้องปรับแก้สมการเพื่อให้เหมาะสม โดยเพิ่มค่าระดับผลกระทบของจุดบกพร่องใดๆ ที่ส่งผลต่อการล่วงละเมิดระบบในสมการข้างต้น ซึ่งทำให้ได้สมการใหม่ ดังนี้

$$W_i = W_{C_i} + W_{I_i} + W_{A_i} + W_{S_i}$$

โดยที่ W_i คือ ความเปราะบางของจุดอ่อนใดๆ

W_{C_i} คือ ความเปราะบางของจุดอ่อนใดๆอันส่งผลต่อการรักษาความลับ โดย

$W_{C_i} = C_i * L_i$; C_i คือ ความเสียหายต่อการรักษาความลับ และ L_i คือ ระดับความรุนแรง

W_{I_i} คือ ความเปราะบางของจุดอ่อนใดๆอันส่งผลต่อการบูรณภาพ โดย

$W_{I_i} = I_i * L_i$; I_i คือ ความเสียหายต่อการรักษาบูรณภาพ และ L_i คือ ระดับความรุนแรง

W_{A_i} คือ ความเปราะบางของจุดอ่อนใดๆอันส่งผลต่อสภาพพร้อมใช้งาน โดย $W_{A_i} = A_i * L_i$; A_i คือ ความเสียหายต่อการรักษาสภาพพร้อมใช้งาน และ L_i คือ ระดับความรุนแรง

W_{S_i} คือ ความเปราะบางของจุดอ่อนใดๆอันส่งผลต่อการล่วงละเมิดระบบ โดย $W_{S_i} = S_i * L_i$; S_i คือ ความเสียหายต่อการล่วงละเมิด และ L_i คือ ระดับความรุนแรง

$$S_i = \sum_{i=1}^{n} (S1_i + S2_i + S3_i + S4_i) ;$$

โดยที่ $S1_i$ คือ ความเสียหายจากการเรียกทำงานชุดคำสั่งใดๆ

$S2_i$ คือ ความเสียหายจากการเพิ่มสิทธิในการทำงาน

$S3_i$ คือ ความเสียหายจากเข้าถึงบัญชีผู้ใช้

$S4_i$ คือ ความเสียหายจากเข้าถึงระดับราก

i คือ ลำดับของซีวีอี

จากสมการดังกล่าว สามารถหาคะแนนความเปราะบางรวมทั้งหมดได้จาก

$$\text{คะแนนความเปราะบางรวมทั้งหมด} = \sum_{i=1}^{n} W_i$$

หรือ

$$\text{คะแนนความเปราะบางรวมทั้งหมด} = \sum_{i=1}^{n} (Ci + Ii + Ai + Si) * Li$$

การกำหนดคะแนนจะกำหนดให้ความเสียหายแต่ละประเภท(C_i, I_i, A_i และ S_i) มีคะแนนเท่ากัน คือ 1 คะแนน สำหรับความเสียหายในลักษณะของการล่วงละเมิดระบบ ซึ่งประกอบไปด้วยลักษณะย่อย 4 ลักษณะ ได้แก่ การเรียกทำงานชุดคำสั่งใดๆ, การเพิ่มสิทธิในการทำงาน, การเข้าถึงบัญชีผู้ใช้ และการเข้าถึงระดับราก จะถือว่าลักษณะย่อยแต่ละลักษณะนั้นมี

คะแนนอย่างละ 0.25 คะแนน และเนื่องจากความเสียหายที่เกิดขึ้นนั้นมีปริมาณความรุนแรงที่แตกต่างกัน จึงได้กำหนดระดับความรุนแรง(L_i) โดยกำหนดให้ความรุนแรงระดับสูงมีค่าเป็น 3 เท่า และความรุนแรงระดับปานกลางมีค่าเป็น 2 เท่าของความรุนแรงในระดับต่ำ ตามลำดับ โดยพื้นฐานการให้คะแนนจะขึ้นอยู่กับการจัดกลุ่มของจุดอ่อนและระบบปฏิบัติการที่ได้รับผลกระทบจากจุดอ่อน ซึ่งหากระบบใดได้ผลคะแนนความเปราะปรางรวมมีค่าสูง นั่นย่อมหมายความว่าระบบนั้นจะมีความเปราะบางและความเสี่ยงต่อการโจมตีซึ่งก่อให้เกิดความเสียหายได้มากกว่าระบบที่มีได้ผลคะแนนความเปราะปรางรวมที่มีค่าน้อย

ในตารางที่ 4.1 แสดงตารางการให้คะแนนแก่จุดอ่อน โดยแยกออกตามลักษณะความเสียหายที่เกิดขึ้น และระดับความรุนแรงของความเสียหายนั้น

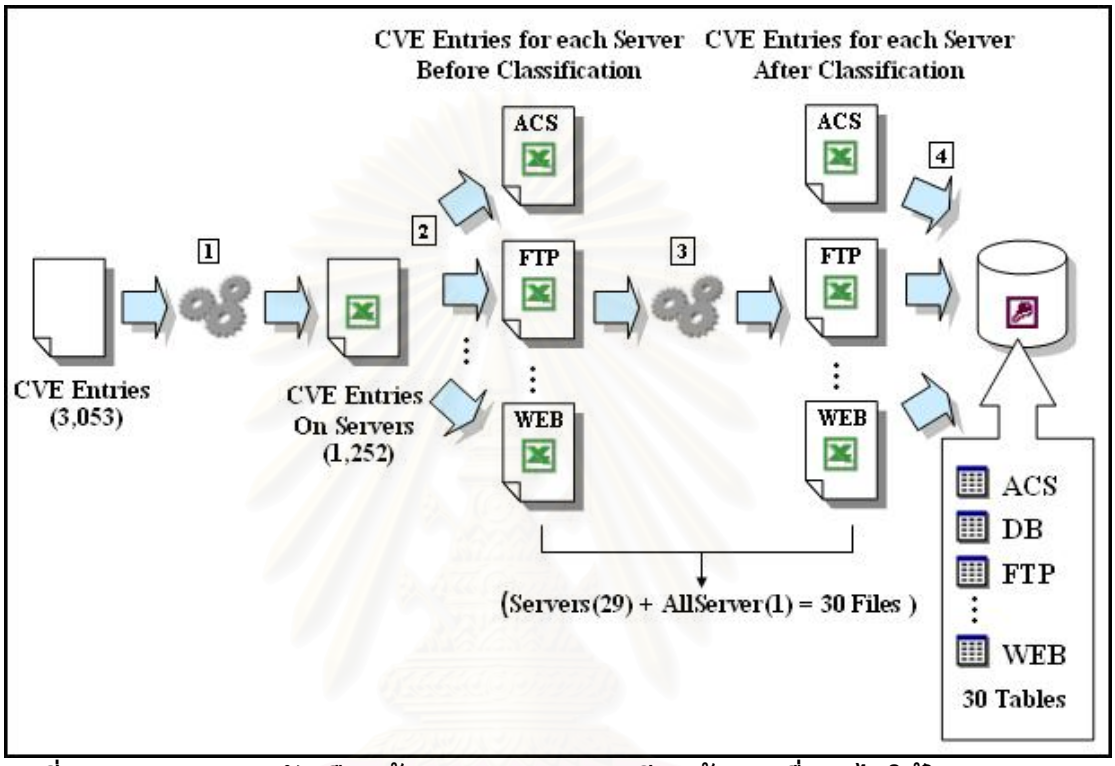
Loss Type	Severity(L_i)		
	High	Medium	Low
Confidentiality(C_i)	3	2	1
Integrity(I_i)	3	2	1
Availability(A_i)	3	2	1
System Compromise (S_i)	3	2	1

System Compromise	Severity		
	High	Medium	Low
Run Arbitrary Code	0.75	0.5	0.25
Elevate Privilege	0.75	0.5	0.25
Account Break-in	0.75	0.5	0.25
Root Break-in	0.75	0.5	0.25

ตารางที่ 4.1 ตารางการให้คะแนนจุดอ่อน

เนื่องจากข้อมูลที่จัดเก็บไว้อยู่ในรูปแบบของแฟ้มข้อมูลเอ็กซ์เซล ทำให้ยากต่อการนับคะแนนและการคำนวณผลรวมคะแนน ดังนั้นการนับคะแนนในงานวิจัยนี้จึงจำเป็นต้องแปลงข้อมูลที่จัดเก็บในแฟ้มข้อมูลเอ็กซ์เซลแต่ละแฟ้มข้อมูลซึ่งก็คือข้อมูลจุดอ่อนของเซิร์ฟเวอร์แต่ละประเภทให้จัดเก็บอยู่ในรูปแบบของตารางในฐานข้อมูล ซึ่งจะมีตารางทั้งหมด 29 ตารางตามจำนวนของประเภทเซิร์ฟเวอร์ที่จะทำการวิเคราะห์ในงานวิจัยนี้ และมีตารางเพิ่มอีก1 ตาราง

สำหรับข้อมูลจุดอ่อนรวมของเซิร์ฟเวอร์ทุกประเภทรวมกัน รวมทั้งสิ้น 30 ตาราง โดยตารางที่จัดเก็บในฐานข้อมูลจะมีโครงสร้างเหมือนกับโครงสร้างตารางในแฟ้มข้อมูลเอ็กซ์เซล เพื่อความง่ายในการแปลงข้อมูลจากนั้นจึงค่อยทำการส่งคำสั่งเรียกค้นเพื่อประมวลผลลัพธ์คะแนนที่ได้ออกมา



รูปที่ 4.1 กระบวนการคัดเลือกข้อมูลจุดอ่อนและเตรียมข้อมูลเพื่อนำไปใช้ในการคำนวณผลต่าง ๆ

จากรูปที่ 4.1 แสดงกระบวนการในการคัดเลือกข้อมูลจุดอ่อนและการเตรียมข้อมูลจุดอ่อนที่ผ่านการคัดเลือกเพื่อใช้ในการคำนวณปริมาณจุดอ่อนและคะแนนความเปราะบางบนเซิร์ฟเวอร์ โดยมีขั้นตอนต่างๆดังต่อไปนี้

1. ในขั้นตอนแรกจะทำการคัดแยกจุดอ่อนจากรายการซีวีอีทั้งหมด 3,053 รายการ โดยกรองเอาเฉพาะจุดอ่อนที่เกิดขึ้นบนซอฟต์แวร์เซิร์ฟเวอร์เท่านั้น ซึ่งหลังจากเสร็จสิ้นกระบวนการคัดเลือกในขั้นตอนนี้แล้วทำให้เหลือจุดอ่อนจากรายการซีวีอีเพียง 1,252 รายการ เท่านั้น โดยจัดเก็บในรูปแบบของแฟ้มข้อมูลเอ็กซ์เซล

2. นำข้อมูลจุดอ่อนจากรายการซีวีอีที่ได้จากขั้นตอนแรกมาทำการแยกออกตามประเภทของเซิร์ฟเวอร์ที่เกิดจุดอ่อนนั้นๆ โดยแยกจัดเก็บข้อมูล 1 แฟ้มข้อมูลเอ็กซ์

เซลต่อประเภทของเซิร์ฟเวอร์ 1 ประเภท ซึ่งจะได้แฟ้มข้อมูลจุดอ่อนของเซิร์ฟเวอร์ประเภทต่างๆ 29 แฟ้มข้อมูล รวมกับแฟ้มข้อมูลจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์ทั้งหมดที่ไม่ได้แยกประเภทของเซิร์ฟเวอร์อีก 1 แฟ้มข้อมูล รวมทั้งสิ้น 30 แฟ้มข้อมูลเอ็กซ์เซล

3. บันทึกข้อมูลรายละเอียดจุดอ่อนที่ลงในตารางจัดเก็บข้อมูลของแต่ละเซิร์ฟเวอร์ตัวอย่างดังในบทที่ 3 ข้อที่ 3.4 โดยรูปแบบตารางที่ใช้ในการจัดเก็บข้อมูลของแต่ละเซิร์ฟเวอร์จะมีโครงสร้างที่เหมือนกันหมดยกเว้นในส่วนของประเภทเซิร์ฟเวอร์ เนื่องจากเซิร์ฟเวอร์บางประเภทอาจมีการแบ่งรายละเอียดย่อยลงไปอีก

4. เนื่องจากข้อมูลในตารางจัดเก็บข้อมูล ซึ่งประกอบไปด้วยข้อมูลจุดอ่อน ข้อมูลที่ได้จากจัดกลุ่มจัดอ่อน และระบบปฏิบัติการที่ได้รับผลกระทบมีอยู่เป็นจำนวนมาก ทำให้การนับจำนวนจุดอ่อนและการคำนวณคะแนนความเปราะบางทำได้ยาก การนับและการให้คะแนนด้วยมืออาจจะทำให้ต้องใช้เวลานานมากและสามารถก่อเกิดความผิดพลาดได้ง่าย ดังนั้นจึงจำเป็นต้องแปลงแฟ้มข้อมูลเอ็กซ์เซลที่ได้ทั้งหมด ให้อยู่ในรูปของตารางในฐานข้อมูลซึ่งจำนวนตารางที่ได้จะมีจำนวนเท่ากับจำนวนของแฟ้มข้อมูลเอ็กซ์เซล คือ 30 ตาราง โดยโครงสร้างของตารางที่ได้จะกำหนดให้มีลักษณะใกล้เคียงกับรูปแบบตารางจัดเก็บข้อมูล ในบทที่ 3 ข้อที่ 3.3 รูปที่ 3.7 – 3.11 มากที่สุด ซึ่งการทำเช่นนี้ มีวัตถุประสงค์เพื่อช่วยให้การคำนวณจำนวนจุดอ่อนและการนับคะแนนความเปราะบางทำได้ง่าย รวดเร็วและมีความถูกต้องมากยิ่งขึ้นเท่านั้น เพราะฉะนั้นตารางแต่ละตารางจึงไม่ได้ผ่านการออกแบบในรูปของตารางความสัมพันธ์ และการทำให้เป็นบรรทัดฐาน(Normalization) ตารางแต่ละตารางถือเป็นอิสระต่อกัน ไม่มีความสัมพันธ์ซึ่งกันและกัน ดังนั้นจึงไม่สามารถเขียนแสดงในรูปแบบของ E/R Diagram ออกมาได้

ในรูปที่ 4.2-4.5 แสดงข้อมูลของตารางที่ 3.5 ในบทที่ 3 หลังจากที่ได้เปลี่ยนรูปแบบจากแฟ้มข้อมูลเอ็กซ์เซลให้อยู่ในรูปแบบของตารางในฐานข้อมูลเรียบร้อยแล้ว ซึ่งโครงสร้างของตารางในฐานข้อมูลที่ได้ สามารถเทียบรูปแบบโครงสร้างได้กับโครงสร้างของตารางจัดเก็บข้อมูลในแฟ้มข้อมูลเอ็กซ์เซลในบทที่ 3 ข้อที่ 3.3 รูปที่ 3.7 – 3.11 แต่มีการตัดเขตข้อมูลบางส่วนที่ไม่เกี่ยวข้องหรือไม่มีความจำเป็นต้องใช้ในการเรียกค้นข้อมูลออกไป และปรับโครงสร้างรูปแบบของหัวตารางที่มีลักษณะเป็นแบบลำดับชั้น(Hierarchy) ให้อยู่ในรูปแบบระนาบ(Flat) ตัวอย่างดัง

แสดงในรูปที่ 4.6 โดยข้อมูลที่จัดเก็บในตารางจัดเก็บข้อมูลของแฟ้มเอ็กซ์เซลเขตข้อมูลใดมีค่าเป็น “/” จะถูกเปลี่ยนค่าเป็น 1 และเขตข้อมูลที่ไม่มีการเก็บค่าใดๆหรือเป็นค่าว่างจะถูกกำหนดให้มีค่าเป็น 0 นอกนั้นให้เก็บค่าคงเดิมไว้เหมือนที่เก็บไว้ในแฟ้มข้อมูลเอ็กซ์เซล

CVE_Name	CVE_DESC	SV_HIGH	SV_MEDIUM	SV_LOW	VT_INPUT	VT_BOUNDARY	VT_ACCESS	VT_SERIAL	VT_CONFIG	VT_ENV	VT_DESIGN	VT_EXCEPT	VT_OTHERS	LC_SYSTEM	LC_MEMORY	LC_PROCESS	LC_DEVICE	LC_FILE	LC_AUTHEN	LC_SUPPORT	LC_APPL	LT_CONFIDENT	LT_INTEGRITY	LT_AVAIL	LT_SP_RUN	LT_SP_ELEVATE	LT_SP_ACCOUNT	LT_SP_ROOT	ER_REMOTE	ER_LOCAL	DB_MSSQL	DB_MSQL	DB_MYSQL
CVE-2001-0344	An SQL query method in Microsoft SQL Server 2000 Gold and 7.0 using Mixed Mode allows local database users to gain privileges by reusing a cached connection of the sa administrator account.	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	1	1	0	0
CVE-2001-0407	Directory traversal vulnerability in MySQL before 3.23.36 allows local users to modify arbitrary files and gain privileges by creating a database whose name starts with .. (dot dot).	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	1	0	0	1	0	0	0	1	0	0	1

รูปที่ 4.2 ตัวอย่างข้อมูลจุดอ่อนที่จัดเก็บในตารางบนฐานข้อมูลของตัวอย่างตารางที่ 3.5#1

DB_ORACLE	DB_OTHER	UX_SOLARIS_SP	UX_SOLARIS_NSP	UX_SOLARIS_VER	UX_SUNOS_SP	UX_SUNOS_NSP	UX_SUNOS_VER	UX_AIX_SP	UX_AIX_NSP	UX_AIX_VER	UX_HPUX_SP	UX_HPUX_NSP	UX_HPUX_VER	UX_IRIX_SP	UX_IRIX_NSP	UX_IRIX_VER	UX_SCO_SP	UX_SCO_NSP	UX_SCO_VER	UX_DGUX_SP	UX_DGUX_NSP	UX_DGUX_VER	UX_FREEBSD_SP	UX_FREEBSD_NSP	UX_FREEBSD_VER	UX_OPENBSD_SP	UX_OPENBSD_NSP	UX_OPENBSD_VER	UX_NETBSD_SP	UX_NETBSD_NSP	UX_NETBSD_VER	UX_NSP	LX_REDHAT_SP	LX_REDHAT_NSP	LX_REDHAT_VER	LX_SUSE_SP	LX_SUSE_NSP	LX_SUSE_VER	LX_KERNEL_SP
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	1	0	2.6, 7.0, 8.0	0	0	0	1	0	4.3, 2.4, 3.3	1	0	11.0, 11.11	0	0	0	0	0	0	0	0	0	1	0	3.5.1, 4.2	1	0	2.6, 2.7, 2.8	0	0	0	0	1	0	5.2 6.2, 7.0	1	0	6.4, 7.0, 7.1	0

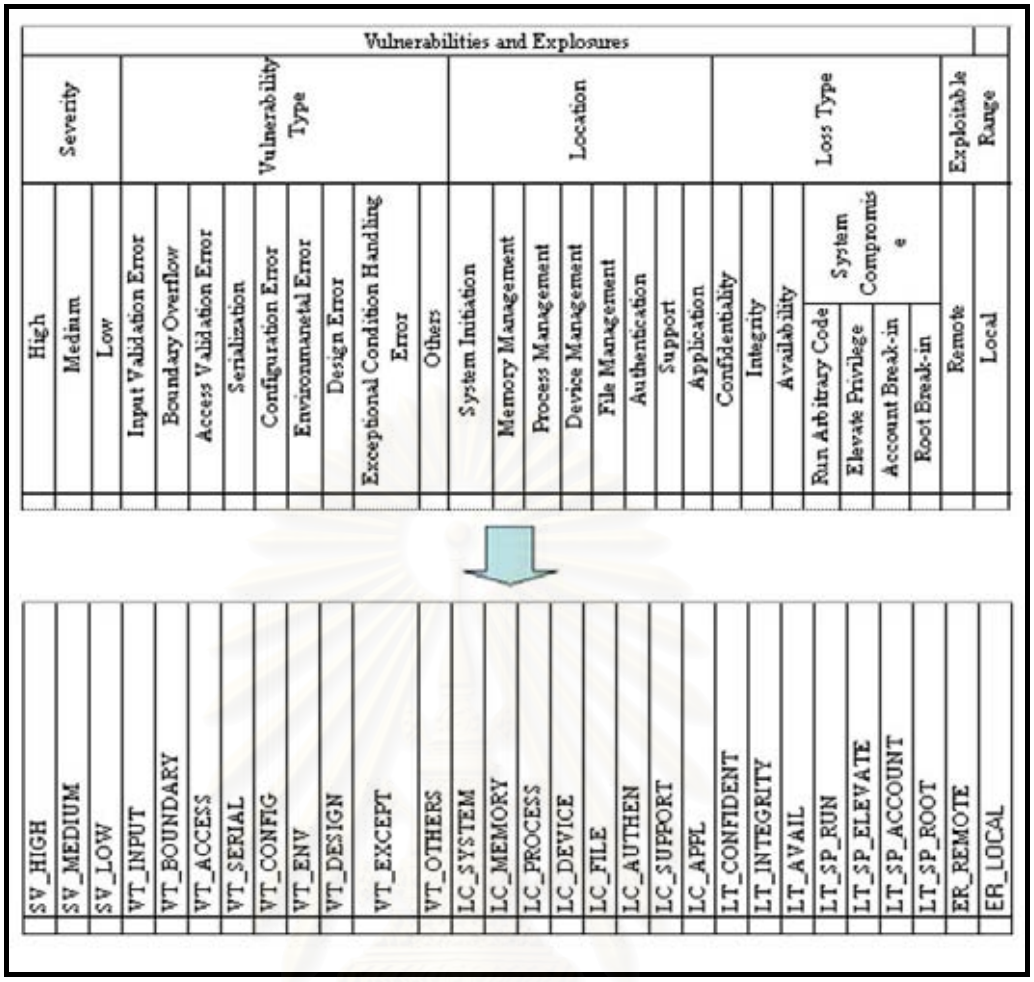
รูปที่ 4.3 ตัวอย่างข้อมูลจุดอ่อนที่จัดเก็บในตารางบนฐานข้อมูลของตัวอย่างตารางที่ 3.5#2

LX_KERNEL_NSP	LX_KERNEL_VER	LX_DEBIAN_SP	LX_DEBIAN_NSP	LX_DEBIAN_VER	LX_MANDRAKE_SP	LX_MANDRAKE_NSP	LX_MANDRAKE_VER	LX_CALDERA_SP	LX_CALDERA_NSP	LX_CALDERA_VER	LX_CONECTIVA_SP	LX_CONECTIVA_NSP	LX_CONECTIVA_VER	LX_TURBO_SP	LX_TURBO_NSP	LX_TURBO_VER	LX_TRUSTIX_SP	LX_TRUSTIX_NSP	LX_TRUSTIX_VER	LX_SLACKWARE_SP	LX_SLACKWARE_NSP	LX_SLACKWARE_VER	LX_NSP	WIN_WIN95	WIN_WIN98	WIN_NT_SP	WIN_NT_NSP	WIN_NT_VER	WIN_NT4SERVER_SP	WIN_NT4SERVER_NSP	WIN_NT4SERVER_VER	WIN_NT4WORK_SP	WIN_NT4WORK_NSP	WIN_NT4WORK_VER	WIN_NT4ENP_SP	WIN_NT4ENP_NSP	WIN_NT4ENP_VER	WIN_NT4TERM_SP	WIN_NT4TERM_NSP
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	4.0,4.0SP1,4.0SP2,4.0SP3,4.0SP4,4.0SP5,4.0SP6,4.0SP6a	0	0	0	0	0	0	0	0	0	0	0
0	0	1	0	2.2	1	0	7.0, 7.1, 7.2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

รูปที่ 4.4 ตัวอย่างข้อมูลจุดอ่อนที่จัดเก็บในตารางบนฐานข้อมูลของตัวอย่างตารางที่ 3.5#3

WIN_NT4TERM_VER	WIN_2000_SP	WIN_2000_NSP	WIN_2000_VER	WIN_2000PRO_SP	WIN_2000PRO_NSP	WIN_2000PRO_VER	WIN_2000SERVER_SP	WIN_2000SERVER_NSP	WIN_2000SERVER_VER	WIN_2000TERM_SP	WIN_2000TERM_NSP	WIN_2000TERM_VER	WIN_2000ADV_SP	WIN_2000ADV_NSP	WIN_2000ADV_VER	WIN_2000DATA_SP	WIN_2000DATA_NSP	WIN_2000DATA_VER	WIN_2003Server_SP	WIN_2003Server_NSP	WIN_2003Server_VER	WIN_XP	WIN_NSP	OS2_WARP_SP	OS2_WARP_NSP	OS2_WARP_VER	NV_NETWARE_SP	NV_NETWARE_NSP	NV_NETWARE_VER	MC_MACOS_SP	MC_MACOS_NSP	MC_MACOS_VER	CC_IOS_SP	CC_IOS_NSP	CC_IOS_VER	NSP
0	0	0	0	1	0	SP1, SP2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

รูปที่ 4.5 ตัวอย่างข้อมูลจุดอ่อนที่จัดเก็บในตารางบนฐานข้อมูลของตัวอย่างตารางที่ 3.5#4



รูปที่ 4.6 ตัวอย่างการแปลงโครงสร้างรูปแบบหัวตารางจากตารางในแฟ้มข้อมูลเอ็กซ์เซลเป็นตารางในฐานข้อมูล

จากรูปที่ 4.6 แสดงตัวอย่างการแปลงโครงสร้างรูปแบบหัวตารางในแฟ้มข้อมูลเอ็กซ์เซลที่มีรูปแบบเป็นลำดับชั้นให้เป็นตารางในฐานข้อมูลโดยมีรูปแบบหัวตารางเป็นแบบระนาบ

4.3 ตัวอย่างการคำนวณคะแนนความเปราะบางจากข้อมูลจุดอ่อน

ในที่นี้จะขอยกตัวอย่างการคำนวณคะแนนความเปราะบาง 2 ตัวอย่าง คือ CVE-1999-0879 และ CVE-2001-0187 ซึ่งเป็นจุดอ่อนที่เกิดขึ้นบนเอฟทีพีเซิร์ฟเวอร์ มีรายละเอียดคร่าวๆ ที่จำเป็นต้องใช้ในการคำนวณ ดังต่อไปนี้

4.3.1 ตัวอย่างที่ 1

CVE Name : CVE-1999-0879

Description : Buffer overflow in WU-FTPD and related FTP servers allows remote attackers to gain root privileges via macro variables in a message file.

Severity : High

Vulnerability Type : Input Validation Error

Location : Memory Management

Loss Type : Root Break-in

Affected Platform :

Linux : Redhat : Version 6.1

Caldera OpenLinux : Not Specified Version

การคำนวณจะให้คะแนนตามกลุ่มของจุดอ่อนและระบบปฏิบัติการที่ได้รับผลกระทบ โดยเทียบกับความเสียหายและระดับความรุนแรง โดยกำหนดค่าเริ่มต้นดังที่กล่าวไว้แล้วใน 4.1 ดังนี้

CVE Name : CVE-1999-0879

Severity : High = 3

Vulnerability Type : Input Validation Error = 1

Location : Memory Management = 1

Loss Type : Root Break-in = 0.25

Affected Platform :

Linux : Redhat : Version 6.1 = 1

Caldera OpenLinux : Not Specified Version = 1

จากนั้นจะคำนวณคะแนนความเปราะบางเพื่อนำผลไปใช้ในการวิเคราะห์ ซึ่งในงานวิจัยนี้จะวิเคราะห์ความเปราะบางในแง่ของประเภทของจุดอ่อน จุดที่เกิดจุดอ่อน และระบบปฏิบัติการที่ได้รับผลกระทบ ซึ่งจากสมการ

$$\text{คะแนนความเปราะบางรวมทั้งหมด} = \sum_{i=1}^{n} (Ci + Ii + Ai + Si) * Li$$

สามารถคำนวณคะแนนความเปราะบางของ CVE-1999-0879 ได้ดังนี้

Vulnerability Type : คะแนนความเปราะบาง = (0 + 0 + 0 + 0.25) * 3 = 0.75

Location : คะแนนความเปราะบาง = (0 + 0 + 0 + 0.25) * 3 = 0.75

OS : Redhat : คะแนนความเปราะบาง = (0 + 0 + 0 + 0.25) * 3 = 0.75

Caldera OpenLinux : คะแนนความเปราะบาง = (0 + 0 + 0 + 0.25) * 3 = 0.75

ผลลัพธ์ที่ได้จะหมายความว่า

1. CVE-1999-0879 มีคะแนนความเปราะบางที่เกิดจากความผิดพลาดในการตรวจสอบข้อมูลนำเข้า 0.75 คะแนน
2. CVE-1999-0879 มีคะแนนความเปราะบางที่เกิดขึ้น ณ ส่วนการจัดการหน่วยความจำ 0.75 คะแนน
3. CVE-1999-0879 มีคะแนนความเปราะบางต่อระบบปฏิบัติการลินุกซ์ 1.5 คะแนน

4.3.2 **ตัวอย่างที่** 2

CVE Name : CVE-2001-0187

Description : Format string vulnerability in wu-ftp 2.6.1 and earlier, when running with debug mode enabled, allows remote attackers to

execute arbitrary commands via a malformed argument that is recorded in a PASV port assignment.

Severity : High

Vulnerability Type : Environmental Error , Exceptional Condition Handling Error

Location : Support

Loss Type : Run Arbitrary Code, Elevate Privilege

Affected Platform :

Unix : HP/UX : Version 11.0,11.11

FreeBSD : Version 4.3

Linux : Redhat : Version 5.2,6.0,6.1,6.2,7.0,7.1,7.2

S.U.S.E Linux : Version 6.1,6.2,6.3,6.4,7.0,7.1,7.2,7.3

Debian Linux : Version 2.2

Mandrake Linux : Version 6.0,6.1,7.0,7.1,7.2,8.0,8.1

Caldera OpenLinux : Version 2.3

Conectiva Linux : Version 4.0,4.1,4.2,5.0,5.1,6.0,7.0,8.0

Turbo Linux : Version 6.0,6.0.1,6.0.2,6.0.3,6.0.4,6.0.5

Slackware Linux : Version 7.0,7.1,8.0

จากสมการ

$$\text{คะแนนความเปราะบางรวมทั้งหมด} = \sum_{i=1}^{n} (Ci + Ii + Ai + Si) * Li$$

ความเปราะบางจากจุดอ่อน CVE-2001-0187 = $(C + I + A + S1 + S2 + S3 + S4) * L$

ซึ่งผลการคำนวณคะแนนความเปราะบางที่ได้เป็นดังนี้

Vulnerability Type :

Environmental Error : คะแนนความเปราะบาง = (0 + 0 + 0 + 0 + 0 + 0.25 + 0.25) * 3 = 1.5

Exceptional Condition Handling Error : คะแนนความเปราะบาง = (0 + 0 + 0 + 0 + 0 + 0.25 + 0.25) * 3 = 1.5

Location : คะแนนความเปราะบาง = (0 + 0 + 0 + 0 + 0 + 0.25 + 0.25) * 3 = 1.5

OS : **Unix** : HP/UX : คะแนนความเปราะบาง = (0 + 0 + 0 + 0 + 0 + 0.25 + 0.25) * 3 = 1.5

FreeBSD : คะแนนความเปราะบาง = (0 + 0 + 0 + 0 + 0 + 0.25 + 0.25) * 3 = 1.5

Linux : Redhat : คะแนนความเปราะบาง = (0 + 0 + 0 + 0 + 0 + 0.25 + 0.25) * 3 = 1.5

S.U.S.E Linux : คะแนนความเปราะบาง = (0 + 0 + 0 + 0 + 0 + 0.25 + 0.25) * 3 = 1.5

Debian Linux : คะแนนความเปราะบาง = (0 + 0 + 0 + 0 + 0 + 0.25 + 0.25) * 3 = 1.5

Mandrake Linux : คะแนนความเปราะบาง = (0 + 0 + 0 + 0 + 0 + 0.25 + 0.25) * 3 = 1.5

Caldera OpenLinux : คะแนนความเปราะบาง = (0 + 0 + 0 + 0 + 0 + 0.25 + 0.25) * 3 = 1.5

Conectiva Linux : คะแนนความเปราะบาง = (0 + 0 + 0 + 0 + 0 + 0.25 + 0.25) * 3 = 1.5

Turbo Linux : คะแนนความเปราะบาง = (0 + 0 + 0 + 0 + 0 + 0.25 + 0.25) * 3 = 1.5

Slackware Linux : คะแนนความเปราะบาง = (0 + 0 + 0 + 0 + 0 + 0.25 + 0.25) * 3 = 1.5

ผลลัพธ์ที่ได้จะหมายความว่า

1. CVE-2001-0187 มีคะแนนความเปราะบางที่เกิดจากความผิดพลาดจากสภาพแวดล้อม 1.5 คะแนน และมีคะแนนความเปราะบางที่เกิดจากความผิดพลาดจากชุดคำสั่งจัดการข้อยกเว้น1.5 คะแนน

2. CVE-2001-0187 มีคะแนนความเปราะบางที่เกิดขึ้น ณ โปรแกรมที่สนับสนุนการทำงานของระบบปฏิบัติการ 1.5 คะแนน

3. CVE-2001-0187 มีคะแนนความเปราะบางต่อระบบปฏิบัติการยูนิกซ์ 3 คะแนน และระบบปฏิบัติการลินุกซ์ 12 คะแนน

การคิดคะแนนความเปราะบางรวมของเซิร์ฟเวอร์จะต้องนำเอาคะแนนความเปราะบางที่คำนวณได้ของซีวีอีที่เกิดขึ้นบนเซิร์ฟเวอร์นั้นๆทั้งหมดมารวมกัน ซึ่งในที่นี้จะยกตัวอย่างการคำนวณคะแนนความเปราะบางรวมโดยการคำนวณจากคะแนนความเปราะบางที่คำนวณได้ของตัวอย่างทั้งสอง ซึ่งหากนำเอาคะแนนความเปราะบางของซีวีอีทั้งสองรายการมารวมกัน จะได้ผลลัพธ์ว่า

1. คะแนนความเปราะบางรวมเมื่อคำนวณตามประเภทของจุดอ่อนจะได้ 3.75 คะแนน (CVE-1999-0879 0.75 คะแนน และ CVE-2001-0187 3 คะแนน)

2. คะแนนความเปราะบางรวมเมื่อคำนวณตามจุดที่เกิดจุดอ่อนจะได้ 2.25คะแนน (CVE-1999-0879 0.75 คะแนน และ CVE-2001-0187 1.5 คะแนน)

3. คะแนนความเปราะบางรวมเมื่อคำนวณตามระบบปฏิบัติการที่ได้รับผลกระทบจากจุดอ่อนจะได้ 16.5 คะแนน แบ่งเป็นยูนิกซ์ 3 คะแนน จาก CVE-2001-0187 และลินุกซ์ 13.5 คะแนน (CVE-1999-0879 1.5 คะแนน และ CVE-2001-0187 12 คะแนน)

จากการคำนวณคะแนนความเปราะบางรวมของตัวอย่างทั้งสอง จะเห็นได้ว่าสามารถรวมคะแนนความเปราะบางของหลายๆซีวีอีในมิติต่างๆได้

ในบทที่ 4 นี้ เป็นหลักเกณฑ์และวิธีการในการคำนวณปริมาณจุดอ่อนและค่าคะแนนความเปราะบางที่เกิดขึ้นของแต่ละซีวีอี พร้อมทั้งยกตัวอย่างการคำนวณคะแนนความเปราะบางและคะแนนความเปราะบางรวม ซึ่งในบทต่อไป คือ บทที่ 5 จะเป็นผลการวิจัย และการวิเคราะห์ผลลัพธ์จากคะแนนความเปราะบางที่คำนวณได้ รวมถึงการเปรียบเทียบผลที่ได้ในแง่มุมต่างๆ

บทที่ 5

ผลการวิจัย

จากการวิจัยโดยใช้ข้อมูลจุดอ่อนในรายการซีวีอีเวอร์ชัน 20040901 จำนวน 3,053 รายการ พบว่ามีรายการจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์เป็นจำนวนทั้งสิ้น 1,252 รายการ แต่เนื่องจากรายการจุดอ่อนที่ถูกคัดเลือกว่าเป็นจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์มีอยู่เป็นจำนวนมาก ทำให้การนับจำนวนจุดอ่อนและการให้คะแนนความเปราะบางโดยการแบ่งกลุ่มของจุดอ่อนและระบบปฏิบัติการที่ได้รับผลกระทบทำได้ยาก และอาจเกิดความผิดพลาดได้ง่าย ในงานวิจัยนี้จึงได้จัดทำเว็บเพจเพื่อช่วยให้การนับข้อมูลจำนวนจุดอ่อนรวมถึงคะแนนความเปราะบางที่เกิดขึ้นสามารถสืบค้นได้ง่ายและถูกต้องมากขึ้น ดังรูปที่ 5.1 ซึ่งการวิเคราะห์ข้อมูลที่ได้สามารถวิเคราะห์ได้หลายมุมมองหลายมิติ(Dimension) ขึ้นอยู่กับว่าผู้ที่จะทำการวิเคราะห์มีความประสงค์ที่จะวิเคราะห์ข้อมูลผลลัพธ์ที่ได้ในแง่มุมใดบ้าง โดยข้อมูลในงานวิจัยที่สามารถนำมาวิเคราะห์แบ่งออกได้เป็น 4 มิติใหญ่ๆ ได้แก่

1. เวลา(ปีที่เกิดจุดอ่อน)
2. การจัดกลุ่มจุดอ่อน
3. ขอบเขตการโจมตี
4. ระบบปฏิบัติการที่ได้รับผลกระทบ

แต่เว็บเพจที่สร้างขึ้นในงานวิจัยนี้จะใช้ในการเรียกค้นข้อมูลเพื่อนำผลที่ได้มาวิเคราะห์เพียง 3 มิติเท่านั้น โดยไม่ได้ยกเอาข้อมูลขอบเขตการโจมตีมาร่วมในการวิเคราะห์ด้วย ซึ่งหากต้องการได้ข้อมูลเพื่อทำการวิเคราะห์ที่มีมิติแตกต่างออกไปจากงานวิจัยนี้ จำเป็นต้องมีการแก้ไขรหัส(Code)ที่ใช้ในการสืบค้นข้อมูลของเว็บเพจดังกล่าว และอาจรวมถึงตารางโครงสร้างข้อมูลที่จัดเก็บไว้ในฐานข้อมูลดังที่กล่าวไว้แล้วในบทที่ 4 ข้อ 4.2 แล้วจึงนำผลที่ได้จากการสืบค้นไปวิเคราะห์ซึ่งอาจอยู่ในรูปแบบของกราฟ หรือข้อมูลตัวเลขตามที่ต้องการ โดยในบทนี้จะยกตัวอย่างตารางแจกแจงผลลัพธ์ที่ได้จากการสืบค้นข้อมูลพร้อมทั้งยกตัวอย่างการวิเคราะห์ข้อมูลจุดอ่อนและความเปราะบางบนเซิร์ฟเวอร์ในมุมมองที่น่าสนใจ ซึ่งมีรายละเอียดต่างๆ ดังต่อไปนี้

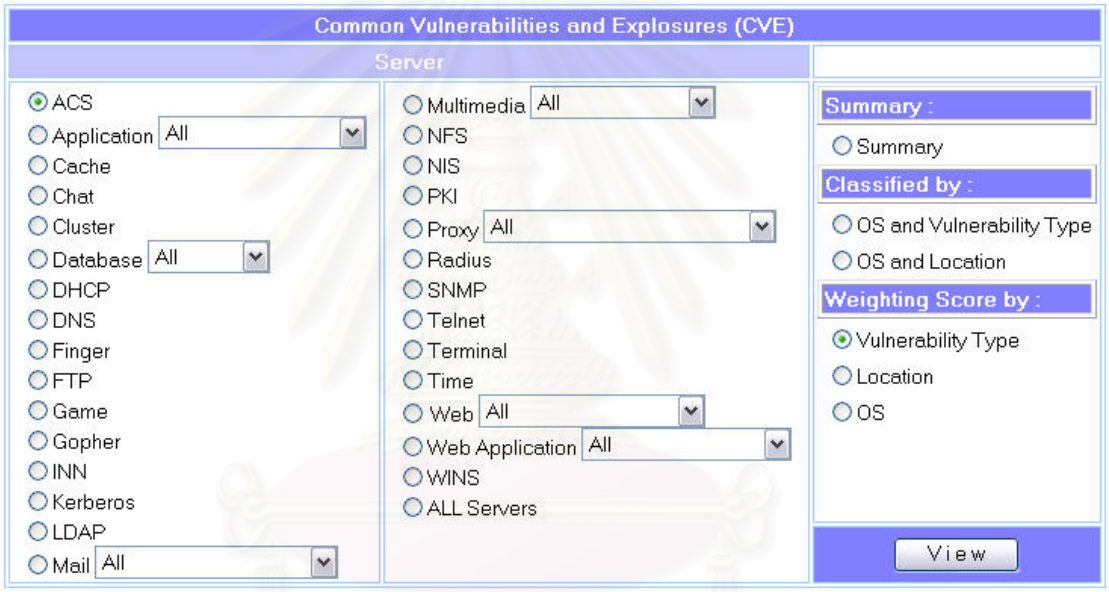
1. ตารางแจกแจงผลลัพธ์ที่ได้จากการเรียกค้นผ่านเว็บเพจ

2. ตัวอย่างการวิเคราะห์และเปรียบเทียบข้อมูลจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์ประเภทต่างๆ

3. ตัวอย่างการวิเคราะห์และเปรียบเทียบความเปราะบางต่อการโจมตีของเซิร์ฟเวอร์ประเภทต่างๆ

4. ตัวอย่างการวิเคราะห์และเปรียบเทียบข้อมูลจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์ของระบบปฏิบัติการประเภทต่างๆ

5. ตัวอย่างการวิเคราะห์และเปรียบเทียบความเปราะบางต่อการโจมตีบนเซิร์ฟเวอร์ของระบบปฏิบัติการประเภทต่างๆ



รูปที่ 5.1 แสดงเว็บเพจสำหรับใช้สืบค้นข้อมูลจำนวนจุดอ่อนและคะแนนความเปราะบางของเซิร์ฟเวอร์

จากรูปที่ 5.1 เว็บเพจที่ใช้สืบค้นข้อมูลจำนวนจุดอ่อนและคะแนนความเปราะบางแบ่งออกได้เป็น 2 ส่วน ส่วนแรกได้แก่ ประเภทของเซิร์ฟเวอร์ ทั้งหมด 29 เซิร์ฟเวอร์ ซึ่งบางเซิร์ฟเวอร์อาจสามารถแยกรายละเอียดย่อยได้อีกขึ้นอยู่กับประเภทของเซิร์ฟเวอร์นั้นๆ และข้อมูลรวมสำหรับเซิร์ฟเวอร์ทุกประเภท ส่วนที่สองได้แก่ ประเภทของตารางแจกแจงข้อมูล 6 แบบ ซึ่งจะกล่าวถึงต่อไปในข้อ 5.1 โดยงานวิจัยนี้ได้นำข้อมูลที่ได้จากการสืบค้นเพียงส่วนหนึ่งมาสร้างเป็นกราฟเพื่อวิเคราะห์ให้เห็นถึงจุดอ่อนและความเปราะบางที่มีอยู่บนเซิร์ฟเวอร์ ทั้งนี้หากต้องการวิเคราะห์ข้อมูลในแง่มุมอื่นก็สามารถทำได้ ขึ้นอยู่กับว่าต้องการวิเคราะห์ข้อมูลในรูปแบบใดและแง่มุมใดบ้าง ซึ่งอาจจะมีรูปแบบที่แตกต่างกันออกไปได้

5.1 ตารางแจกแจงผลลัพธ์ที่ได้

ผลลัพธ์ที่ได้จากการสืบค้นข้อมูลจะอยู่ในรูปของตารางแจกแจงข้อมูลผลลัพธ์ ซึ่งจะมีอยู่ทั้งหมด 6 ตารางด้วยกัน แบ่งเป็น

1. ตารางสรุปจำนวนจุดอ่อนที่เกิดขึ้นโดยแบ่งแยกตามการจัดกลุ่มจุดอ่อน, ระบบปฏิบัติการที่ได้รับผลกระทบ และปีที่เกิดจุดอ่อนนั้นๆ ดังตารางที่ 5.1

2. ตารางแจกแจงจุดอ่อนของเซิร์ฟเวอร์ตามระบบปฏิบัติการเทียบกับประเภทของจุดอ่อนและระดับความรุนแรงที่เกิดขึ้น แยกตามปีที่เกิดจุดอ่อน ในตารางที่ 5.2 แสดงตัวอย่างตารางของจุดอ่อนที่เกิดขึ้นในปี 1999

3. ตารางแจกแจงจุดอ่อนของเซิร์ฟเวอร์ตามระบบปฏิบัติการเทียบกับจุดที่เกิดจุดอ่อนและระดับความรุนแรงที่เกิดขึ้น แยกตามปีที่เกิดจุดอ่อน ดังตารางที่ 5.3 แสดงตัวอย่างตารางของจุดอ่อนที่เกิดขึ้นในปี 1999

4. ตารางแจกแจงคะแนนความเปราะบางของเซิร์ฟเวอร์ตามประเภทของจุดอ่อน แยกตามปีที่เกิดจุดอ่อน ดังตารางที่ 5.4

5. ตารางแจกแจงคะแนนความเปราะบางของเซิร์ฟเวอร์ตามจุดที่เกิดจุดอ่อน แยกตามปีที่เกิดจุดอ่อน ดังตารางที่ 5.5

6. ตารางแจกแจงคะแนนความเปราะบางของเซิร์ฟเวอร์ตามระบบปฏิบัติการที่ได้รับผลกระทบ แยกตามปีที่เกิดจุดอ่อน ดังตารางที่ 5.6

Server : All Servers : The Number of CVE Entries = 1252									
Year				1999	2000	2001	2002	2003	2004	Total
CVE Entries				292	385	256	261	27	31	1252
				The Number of Vulnerabilities						
Vulnerabilities and Explosures	Severity		High	135	118	118	156	14	21	562
			Medium	146	244	134	81	8	5	618
			Low	8	23	4	24	5	5	69
	Vulnerability Type		Input Validation Error	132	125	134	148	14	19	572
			Boundary Overflow	16	53	18	6	3	1	97
			Access Validation Error	39	72	16	20	5	4	156
			Serialization	6	5	10	3	0	0	24
			Configuration Error	61	31	13	11	0	1	117
			Environmental Error	14	2	5	1	0	0	22
			Design Error	19	49	54	67	3	3	195
			Exceptional Condition Handling Error	12	53	29	25	4	3	126
			Others	13	7	1	5	0	3	29
	Location		System Initiation	27	30	14	12	0	4	87
			Memory Management	60	75	37	55	2	6	235
			Process Management	16	24	17	13	2	1	73
			Device Management	7	14	3	6	1	0	31
			File Management	40	72	57	31	1	2	203
			Authentication	10	19	14	21	0	1	65
			Support	86	82	76	77	13	7	341
			Application	40	69	38	46	8	10	211
	Loss Type		Confidentiality	81	144	77	62	7	6	377
			Integrity	41	61	46	59	5	9	221
			Availability	79	140	83	88	8	9	407
		System Compromise	Run Arbitrary Code	40	47	48	90	9	12	246
			Elevate Privilege	9	14	19	32	2	0	76
			Account Break-in	42	33	20	14	2	3	114
			Root Break-in	61	30	43	31	2	6	173
	Exploitable Range		Remote	252	350	215	234	25	30	1106
			Local	53	101	54	34	2	2	246
Affected Platform	Unix		Solaris	37	66	44	26	9	2	184
			SunOS	10	2	2	0	1	0	15
			AIX	28	32	29	20	1	1	111
			HP-UX	34	38	31	18	4	4	129
			IRIX	32	18	16	11	2	2	81
			SCO Unix	9	17	8	4	1	0	39
			DG/UX	13	13	8	4	2	1	41
			FreeBSD	12	19	24	17	2	1	75
			OpenBSD	4	3	9	5	1	1	23
			NetBSD	4	7	7	6	1	1	26
			Not Specified (Unix)	21	9	8	44	7	8	97
	Linux		Redhat	32	32	48	40	3	3	158
			S.U.S.E Linux	2	15	27	27	1	3	75
			Linux Kernel	4	17	10	2	0	0	33
			Debian Linux	5	10	38	41	5	3	102
			Mandrake Linux	0	10	39	31	3	4	87
			Caldera OpenLinux	13	7	24	24	2	1	71
			Conectiva Linux	0	4	23	28	4	3	62
			Turbo Linux	0	2	7	4	1	3	17
			Trustix Secure Linux	0	0	11	20	1	3	35
			SlackwareLinux	1	1	10	6	0	2	20
			Not Specified (Linux)	17	22	20	45	13	11	128
	Windows		Win95	23	57	31	26	2	0	139
			Win98	21	61	32	31	2	0	147
			WinNT	77	158	67	59	3	1	365
			WinNT (Server 4.0)	3	1	1	14	2	0	21
			WinNT (Workstation 4.0)	2	0	1	15	1	0	19
			WinNT (Enterprise Server 4.0)	2	1	0	15	2	0	20
			WinNT (Terminal Server 4.0)	3	0	2	13	2	0	20
			Win2000	32	49	47	61	4	2	195
			Win2000 (Professional)	7	45	34	24	2	0	112
			Win2000 (Server)	0	7	16	23	1	0	47
			Win2000 (Terminal Services)	0	0	0	5	0	0	5
			Win2000 (Advanced Server)	1	8	14	22	2	0	47
			Win2000 (Data Center Server)	0	7	7	21	1	0	36
			Win2003 (Server)	18	17	11	18	2	1	67
			WinXP	17	13	12	35	3	0	80
			Not Specified (Windows)	6	7	8	61	12	8	102
	OS2Warp			0	3	10	4	0	0	17
	Novell (Netware)			3	9	3	3	1	0	19
	MacOS			3	9	15	17	10	3	57
	CISCO (IOS)			3	2	6	2	0	0	13
	CacheOS			0	0	0	1	0	0	1
	Not Specified OS			100	123	68	36	1	9	337

ตารางที่ 5.1 สรุปจำนวนจุดอ่อนที่เกิดขึ้นโดยแบ่งแยกตามการจัดกลุ่มจุดอ่อน,ระบบปฏิบัติการที่ได้รับผลกระทบ และปีที่เกิดจุดอ่อนนั้น ๆ

Server : All Servers The Number of CVE Entries : 1252

Platform	OS	Vulnerability Type 1999																																						Sum
		Input Validation Error				Boundary Overflow				Access Validation Error				Serialization				Configuration Error				Environmental Error				Design Error				Exceptional Condition Handling Error				Others							
		High	Medium	Low	Sum	High	Medium	Low	Sum	High	Medium	Low	Sum	High	Medium	Low	Sum	High	Medium	Low	Sum	High	Medium	Low	Sum	High	Medium	Low	Sum	High	Medium	Low	Sum	High	Medium	Low	Sum				
Unix		83	26	0	109	0	11	1	12	2	8	1	11	12	1	0	13	21	23	4	48	1	3	0	4	4	0	0	4	0	1	0	1	10	3	0	13	215			
	Solaris	15	6	0	21	0	2	1	3	1	2	0	3	1	0	0	1	2	4	1	7	0	1	0	1	0	0	0	0	0	1	0	1	1	0	0	1	38			
	SunOS	3	0	0	3	0	0	0	0	1	1	0	2	0	1	0	1	1	1	0	2	0	1	0	1	1	0	0	1	0	0	0	0	1	1	0	2	12			
	AIX	13	4	0	17	0	2	0	2	0	1	1	2	2	0	0	2	2	3	0	5	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	29			
	HP-UX	13	5	0	18	0	2	0	2	0	2	0	2	2	0	0	2	2	4	0	6	0	0	0	0	1	0	0	1	0	0	0	0	1	2	0	3	34			
	IRIX	15	4	0	19	0	2	0	2	0	1	0	1	2	0	0	2	3	3	1	7	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	2	33			
	SCO Unix	3	1	0	4	0	1	0	1	0	0	0	0	1	0	0	1	1	1	0	2	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	9			
	DG/UX	6	1	0	7	0	2	0	2	0	0	0	0	1	0	0	1	1	1	1	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	13			
	FreeBSD	5	2	0	7	0	0	0	0	0	0	0	0	1	0	0	1	2	1	1	4	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	13			
	OpenBSD	2	0	0	2	0	0	0	0	0	0	0	0	1	0	0	1	1	1	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5			
	NetBSD	1	0	0	1	0	0	0	0	0	0	0	0	1	0	0	1	1	1	0	2	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	5			
	Not Specified	7	3	0	10	0	0	0	0	0	1	0	1	0	0	0	0	5	3	0	8	1	0	0	1	2	0	0	2	0	0	0	0	2	0	0	2	24			
Linux		43	6	0	49	0	4	0	4	2	2	0	4	2	0	0	2	3	8	1	12	2	0	0	2	0	1	0	1	0	0	0	0	2	1	0	3	77			
	Red Hat	20	3	0	23	0	2	0	2	2	1	0	3	0	0	0	0	0	2	1	3	1	0	0	1	0	0	0	0	0	0	0	0	1	0	0	1	33			
	S.U.S.E Linux	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	2			
	Linux Kernel	1	2	0	3	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5			
	Debian Linux	2	1	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	1	0	1	6			
	Mandrake Linux	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
	Caldera OpenLinux	10	0	0	10	0	2	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	13			
	Conectiva Linux	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
	Turbo Linux	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
	Trustix Secure Linux	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
	Slackware Linux	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1			
	Not Specified	8	0	0	8	0	0	0	0	0	1	0	1	2	0	0	2	2	4	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	17			
Windows		51	48	0	99	0	22	0	22	4	20	0	24	6	1	0	7	11	28	5	44	6	9	0	15	2	8	0	10	0	6	4	10	6	4	0	10	241			
	Win95	8	7	0	15	0	2	0	2	0	2	0	2	1	0	0	1	2	0	1	3	1	0	0	1	0	0	0	0	0	1	0	1	1	0	0	1	26			
	Win98	6	7	0	13	0	3	0	3	0	2	0	2	1	0	0	1	2	0	1	3	1	0	0	1	0	0	0	0	0	1	0	1	1	0	0	1	25			
	WinNT	18	15	0	33	0	9	0	9	3	5	0	8	1	1	0	2	3	12	1	16	1	4	0	5	1	4	0	5	0	4	1	5	1	2	0	3	86			
	WinNT4.0 Server	0	1	0	1	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3			
	WinNT4.0 Workstation	0	1	0	1	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2			
	WinNT4.0 Enterprise Server	0	1	0	1	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2			
	WinNT4.0 Terminal Server	0	1	0	1	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	3			
	Win2000	6	4	0	10	0	3	0	3	1	3	0	4	1	0	0	1	1	7	1	9	1	3	0	4	1	3	0	4	0	0	1	1	1	1	0	2	38			
	Win2000 Professional	2	3	0	5	0	0	0	0	0	1	0	1	0	0	0	0	1	1	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8			
	Win2000 Server	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
	Win2000 Terminal Services	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
	Win2000 Advanced Server	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1			
	Win2000 Data Center Server	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
	Win2003 Server	5	2	0	7	0	2	0	2	0	1	0	1	1	0	0	1	1	4	0	5	1	1	0	2	0	1	0	1	0	0	1	1	1	0	0	1	21			
	WinXP	5	2	0	7	0	2	0	2	0	2	0	2	1	0	0	1	1	2	1	4	1	1	0	2	0	0	0	0	0	0	1	1	1	0	0	1	20			
	Not Specified	1	4	0	5	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6			
OS2	OS2Warp	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
Novell	Netware	0	0	0	0	0	0	0	0	0	1	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	2	0	0	0	0	4			
MacOS	MacOS	1	0	0	1	0	0	0	0	0	0	0	0	1	0	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3			
CISCO	IOS	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	2	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	3			
CacheOS	CacheOS	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
Not Specified		25	15	1	41	0	3	0	3	7	12	1	20	0	1	0	1	12	13	0	25	1	4	0	5	4	3	1	8	1	4	0	5	1	1	0	2	110			
Total Number of Vulnerabilities		203	95	1	299	0	40	1	41	15	43	2	60	23	4	0	27	48	72	10	130	10	16	0	26	11	12	1	24	2	12	4	18	19	9	0	28	653			

ตารางที่ 5.2 ตัวอย่างตารางแจกแจงจุดอ่อนของเซิร์ฟเวอร์ตามระบบปฏิบัติการเทียบกับประเภทของจุดอ่อนที่เกิดขึ้นในปี 1999

Server : All Servers The Number of CVE Entries : 1252																																				
Platform	OS	Location																																		
		1999																																		
		System Initiation				Memory Management				Process Management				Device Management				File Management				Authentication				Support				Application				Sum
		High	Medium	Low	Sum	High	Medium	Low	Sum	High	Medium	Low	Sum	High	Medium	Low	Sum	High	Medium	Low	Sum	High	Medium	Low	Sum	High	Medium	Low	Sum	High	Medium	Low	Sum	
Unix		4	2	4	10	25	9	0	34	10	5	0	15	0	8	0	8	4	15	1	20	6	0	0	6	56	25	0	81	16	11	1	28	202
	Solaris	0	0	1	1	7	2	0	9	2	1	0	3	0	2	0	2	1	3	0	4	1	0	0	1	7	6	0	13	1	2	1	4	37
	SunOS	0	1	0	1	0	0	0	0	0	1	0	1	0	0	0	0	0	1	0	1	0	0	0	0	5	0	0	5	1	1	0	2	10
	AIX	1	0	0	1	5	1	0	6	2	1	0	3	0	1	0	1	1	2	1	4	1	0	0	1	6	4	0	10	1	1	0	2	28
	HP-UX	0	0	0	0	4	2	0	6	2	1	0	3	0	2	0	2	1	2	0	3	1	0	0	1	9	6	0	15	1	2	0	3	33
	IRIX	0	0	1	1	4	1	0	5	2	0	0	2	0	1	0	1	1	1	0	2	1	0	0	1	9	5	0	14	3	2	0	5	31
	SCO Unix	0	0	0	0	1	1	0	2	1	0	0	1	0	1	0	1	0	1	0	1	0	0	0	0	4	0	0	4	0	0	0	0	9
	DG/UX	0	0	1	1	1	1	0	2	1	0	0	1	0	0	0	0	0	1	0	1	1	0	0	1	5	2	0	7	0	0	0	0	13
	FreeBSD	1	1	1	3	1	0	0	1	0	0	0	0	0	1	0	1	0	1	0	1	0	0	0	0	3	0	0	3	2	1	0	3	12
	OpenBSD	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	2	1	1	0	2	4
	NetBSD	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	2	1	1	0	2	4
	Not Specified	2	0	0	2	2	1	0	3	0	1	0	1	0	0	0	0	0	3	0	3	1	0	0	1	4	2	0	6	5	0	0	5	21
Linux		2	3	1	6	23	2	0	25	2	0	0	2	0	1	0	1	1	4	0	5	0	1	0	1	19	10	0	29	4	1	0	5	74
	Red Hat	0	1	1	2	12	1	0	13	1	0	0	1	0	0	0	0	1	1	0	2	0	1	0	1	8	4	0	12	1	0	0	1	32
	S.U.S.E Linux	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	0	1	2
	Linux Kernel	0	1	0	1	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	2	4
	Debian Linux	0	0	0	0	2	0	0	2	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	2	0	2	0	0	0	0	5
	Mandrake Linux	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Caldera OpenLinux	0	0	0	0	6	1	0	7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	2	0	6	0	0	0	0	13
	Conectiva Linux	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Turbo Linux	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Trustix Secure Linux	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Slackware Linux	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	1
	Not Specified	2	1	0	3	3	0	0	3	1	0	0	1	0	0	0	0	0	2	0	2	0	0	0	0	5	2	0	7	1	0	0	1	17
Windows		1	4	5	10	24	41	4	69	13	9	0	22	0	11	0	11	1	33	0	34	2	4	0	6	9	25	0	34	19	8	0	27	213
	Win95	0	0	1	1	3	6	0	9	2	0	0	2	0	1	0	1	0	4	0	4	0	0	0	0	1	1	0	2	4	0	0	4	23
	Win98	0	0	1	1	2	6	0	8	2	0	0	2	0	1	0	1	0	5	0	5	0	0	0	0	1	1	0	2	3	0	0	3	22
	WinNT	1	1	1	3	8	14	1	23	3	6	0	9	0	3	0	3	1	12	0	13	1	1	0	2	5	12	0	17	5	2	0	7	77
	WinNT4.0 Server	0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	3
	WinNT4.0 Workstation	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	2
	WinNT4.0 Enterprise Server	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	2
	WinNT4.0 Terminal Server	0	0	0	0	0	1	0	1	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	3
	Win2000	0	0	1	1	4	4	1	9	2	2	0	4	0	1	0	1	0	5	0	5	0	1	0	1	2	5	0	7	2	2	0	4	32
	Win2000 Professional	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	3	0	3	1	0	0	1	0	1	0	1	1	0	0	1	7
	Win2000 Server	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Win2000 Terminal Services	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Win2000 Advanced Server	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
	Win2000 Data Center Server	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Win2003 Server	0	1	0	1	3	3	1	7	2	0	0	2	0	0	0	0	0	2	0	2	0	1	0	1	0	1	0	1	2	2	0	4	18
	WinXP	0	1	1	2	3	3	1	7	2	0	0	2	0	1	0	1	0	1	0	1	0	1	0	1	0	0	0	0	2	1	0	3	17
	Not Specified	0	0	0	1	3	0	4	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	1	0	1	6
OS2	OS2Warp	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Novell	Netware	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	1	0	0	1	0	0	0	0	0	1	0	1	0	0	0	0	3
MacOS	MacOS	1	0	0	1	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	3
CISCO	IOS	1	0	0	1	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	3
CacheOS	CacheOS	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Not Specified		6	8	0	14	7	5	0	12	0	2	0	2	0	3	0	3	5	10	1	16	4	2	0	6	14	11	1	26	10	9	1	20	99
Total Number of Vulnerabilities		15	17	10	42	79	57	4	140	28	16	0	44	0	23	0	23	12	62	2	76	12	7	0	19	99	73	1	173	49	29	2	80	597

ตารางที่ 5.3 ตัวอย่างตารางแจกแจงจุดอ่อนของเซิร์ฟเวอร์ตามระบบปฏิบัติการเทียบกับจุดที่เกิดจุดอ่อนและระดับความรุนแรงที่เกิดขึ้นในปี 1999

Server : All Servers The Number of CVE Entries : 1252						
No.	Vulnerability Type	Loss Type				
		1999				
		Confidentiality	Integrity	Availability	System Compromise	Sum
1	Input Validation Error	40	20	100	72.25	232.3
2	Boundary Condition Error	9	0	24	0	33
3	Access Validation Error	32	21	7	12	72
4	Serialization	7	0	4	1.5	12.5
5	Configuration Error	62	43	10	16.75	131.8
6	Environmental Error	13	7	12	1.5	33.5
7	Design Error	15	10	8	6	39
8	Exceptional Handling Error	2	0	17	1.5	20.5
9	Others	16	10	4	3	33
Total Number of Weighting Scores		196	111	186	114.5	607.5

ตารางที่ 5.4 **ตัวอย่างตารางแจกแจงคะแนนความเปราะบางของเซิร์ฟเวอร์ตามประเภทของจุดอ่อนที่เกิดขึ้นในปี** 1999

จากตารางที่ 5.4 แสดงคะแนนความเปราะบางของเซิร์ฟเวอร์โดยเปรียบเทียบความเปราะบางจากประเภทของจุดอ่อนออกตามลักษณะความเสียหายที่เกิดขึ้น ซึ่งคะแนนจากตารางทำให้วิเคราะห์ได้ว่าในปี 1999 จุดที่เป็นจุดอ่อนต่อการโจมตีบนเซิร์ฟเวอร์มากที่สุด ได้แก่ การตรวจสอบข้อมูลนำเข้า

Server : All Servers The Number of CVE Entries : 1252						
No.	Location	Loss Type				
		1999				
		Confidentiality	Integrity	Availability	System Compromise	Sum
1	System Initialization	20	23	12	9.25	64.25
2	Memory Management	2	5	83	29.5	119.5
3	Process Management	4	0	26	3	33
4	Device Management	2	0	14	0	16
5	File Management	53	24	5	4	86
6	Authentication	4	5	0	5.5	14.5
7	Support	45	20	29	38	132
8	Application	43	12	2	17	74
Total Number of Weighting Scores		173	89	171	106.25	539.3

ตารางที่ 5.5 **ตัวอย่างตารางแจกแจงคะแนนความเปราะบางของเซิร์ฟเวอร์ตามจุดที่เกิดจุดอ่อนที่เกิดขึ้นในปี** 1999

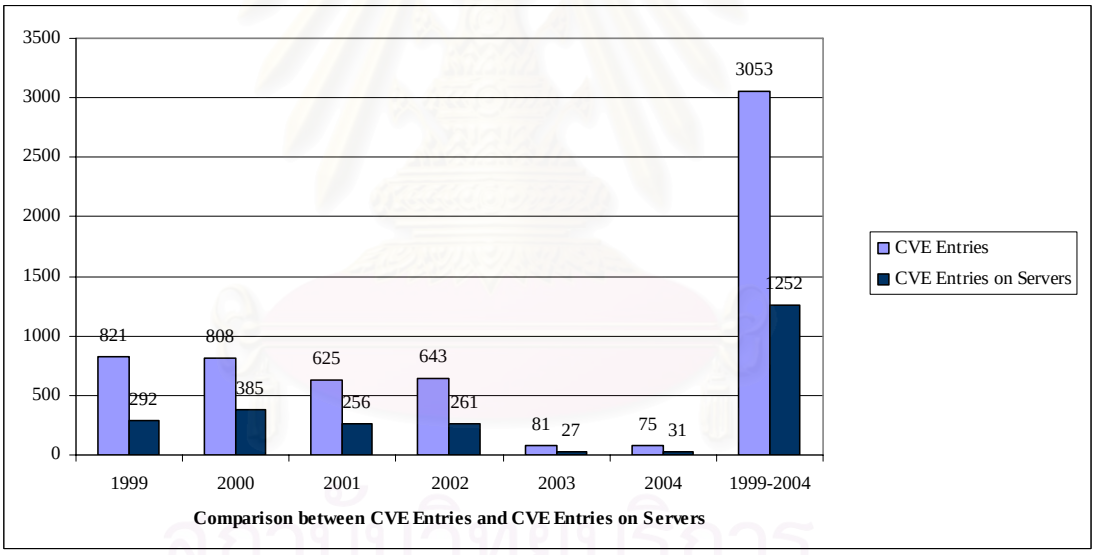
จากตารางที่ 5.5 แสดงคะแนนความเปราะบางของเซิร์ฟเวอร์โดยเปรียบเทียบความเปราะบางจากจุดที่เกิดจุดอ่อนในปี 1999 ซึ่งทำให้ทราบได้ว่าในปีดังกล่าวการโจมตีระบบมักเน้นการโจมตีไปที่โปรแกรมที่สนับสนุนการทำงานของระบบปฏิบัติการ และการจัดการหน่วยความจำ

Server : All Servers The Number of CVE Entries : 1252						
Platform	Operting System	Loss Type				
		1999				
		Confidentiality	Integrity	Availability	System Compromise	Sum
Unix		96	38	140	93.75	367.75
	Solaris	13	4	30	16.25	63.25
	SunOS	3	2	4	5.5	14.5
	AIX	8	5	26	14	53
	HP-UX	14	4	32	14.25	64.25
	IRIX	17	7	21	14	59
	SCO Unix	5	2	4	4.5	15.5
	DG/UX	3	0	4	7.25	14.25
	FreeBSD	4	2	9	6	21
	OpenBSD	3	2	0	2.25	7.25
	NetBSD	6	2	0	1.5	9.5
	Not Specified	20	8	10	8.25	46.25
Linux		26	20	36	47.25	129.25
	Red Hat	10	9	25	19.5	63.5
	S.U.S.E Linux	3	3	0	0.75	6.75
	Linux Kernel	0	2	4	0.75	6.75
	Debian Linux	2	2	0	2.75	6.75
	Mandrake Linux	0	0	0	0	0
	Caldera OpenLinux	2	2	7	11.25	22.25
	Conectiva Linux	0	0	0	0	0
	Turbo Linux	0	0	0	0	0
	Trustix Secure Linux	0	0	0	0	0
	Slackware Linux	0	0	0	0.75	0.75
	Not Specified	9	2	0	11.5	22.5
Windows		131	55	182	62	430
	Win95	12	6	14	10	42
	Win98	14	6	14	8.5	42.5
	WinNT	48	18	72	19.5	157.5
	WinNT4.0 Server	0	0	6	0	6
	WinNT4.0 Workstation	0	0	4	0	4
	WinNT4.0 Enterprise Server	0	0	4	0	4
	WinNT4.0 Terminal Server	0	0	6	0	6
	Win2000	23	10	23	8.75	64.75
	Win2000 Professional	6	3	4	2.75	15.75
	Win2000 Server	0	0	0	0	0
	Win2000 Terminal Services	0	0	0	0	0
	Win2000 Advanced Server	0	0	2	0	2
	Win2000 Data Center Server	0	0	0	0	0
	Win2003 Server	13	6	12	5.75	36.75
	WinXP	11	6	12	6	35
	Not Specified	4	0	9	0.75	13.75
OS2	OS2Warp	0	0	0	0	0
Novell	Netware	2	0	0	1.5	3.5
MacOS	MacOS	0	0	0	2.25	2.25
CISCO	IOS	0	3	2	1.5	6.5
CacheOS	CacheOS	0	0	0	0	0
Not Specified		74	46	30	34.75	184.75
Total Number of Weighting Scores		329	162	390	243	1124

ตารางที่ 5.6 ตัวอย่างตารางแจกแจงคะแนนความเปราะบางของเซิร์ฟเวอร์ตามระบบปฏิบัติการที่ได้รับผลกระทบที่เกิดขึ้นในปี 1999

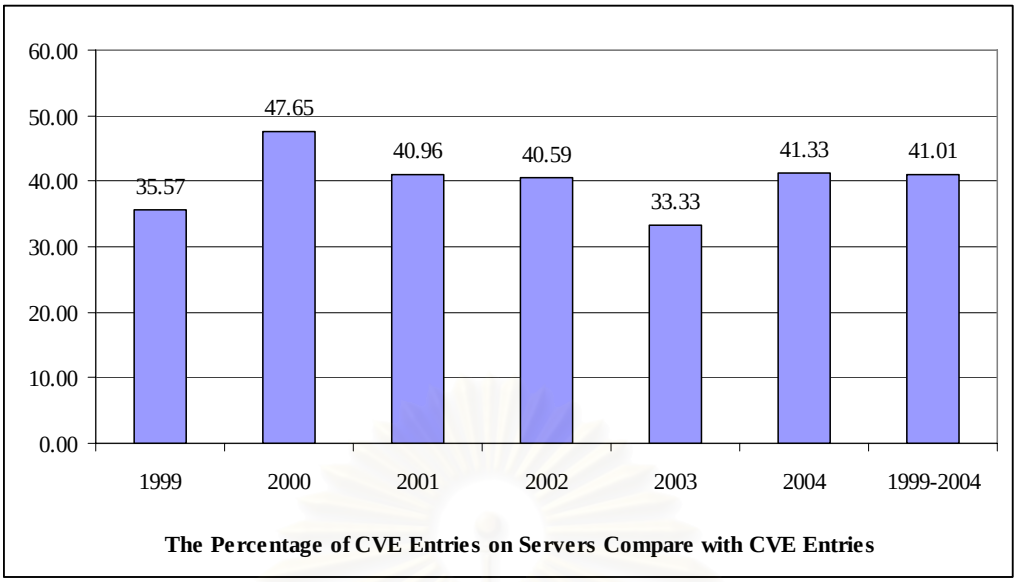
จากตารางที่ 5.6 แสดงคะแนนความเปราะบางของเซิร์ฟเวอร์โดยเปรียบเทียบความเปราะบางจากระบบปฏิบัติการที่ได้รับผลกระทบ ซึ่งจากตัวอย่างข้อมูลในปี 1999 แสดงให้เห็นว่าในปีดังกล่าว เซิร์ฟเวอร์ที่มีโอกาสเสี่ยงต่อการโจมตีมากที่สุดคือ เซิร์ฟเวอร์ที่ทำงานอยู่ภายใต้ระบบปฏิบัติการวินโดวส์ ซึ่งคะแนนความเปราะบางที่ได้ คือ 430 คะแนน โดยระบบปฏิบัติการวินโดวส์ที่ได้รับการโจมตีมากที่สุด คือ วินโดวส์เอ็นที ระบบปฏิบัติการที่มีคะแนนเป็นอันดับ 2 คือ ระบบปฏิบัติการยูนิกซ์ โดยเฉพาะอย่างยิ่ง HP-UX ทีมีคะแนนความเปราะบาง 64.25 คะแนน ส่วนระบบปฏิบัติการลินุกซ์มีความเปราะบางต่อการโจมตีเป็นอันดับที่ 3 โดย Red Hat Linux เป็นระบบปฏิบัติการของลินุกซ์ที่เสี่ยงต่อการโจมตีได้มากที่สุด

เมื่อพิจารณาจำนวนจุดอ่อนที่เกิดขึ้นในแต่ละปีตั้งแต่ปี 1999-2004 จากตารางที่ 5.1 โดยนำมาสร้างกราฟเพื่อเปรียบเทียบกับจำนวนจุดอ่อนที่ปรากฏในรายการซีวีอี จะเห็นว่า จำนวนจุดอ่อนที่มีปรากฏอยู่ในรายการซีวีอีและจำนวนจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์มีแนวโน้มลดลงในแต่ละปี เช่นเดียวกัน ดังแสดงในรูปที่ 5.2



รูปที่ 5.2 กราฟเปรียบเทียบจำนวนจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์กับจำนวนจุดอ่อนในรายการซีวีอี

แต่หลังจากนำข้อมูลดังกล่าวมาเปรียบเทียบกัน โดยคิดเป็นอัตราส่วนร้อยละของจำนวนจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์ต่อจำนวนจุดอ่อนที่ปรากฏอยู่ในรายการซีวีอี จะพบว่าถึงแม้จำนวนจุดอ่อนที่เกิดขึ้นดังกล่าวทั้งสองส่วนมีแนวโน้มที่ลดลง แต่อัตราส่วนจำนวนการเกิดจุดอ่อนบนเซิร์ฟเวอร์เมื่อเทียบกับจำนวนจุดอ่อนตามรายการซีวีอียังคงมีอัตราการส่วนที่ไม่เปลี่ยนแปลงมากนัก โดยมีอัตราการส่วนในแต่ละปีอยู่ในช่วงร้อยละ 33.33-47.65 และอัตราส่วนเฉลี่ยอยู่ที่ร้อยละ 41.01 ดังแสดงในรูปที่ 5.3



รูปที่ 5.3 กราฟแสดงอัตราส่วนเป็นร้อยละของจำนวนจุดอ่อนบนเซิร์ฟเวอร์เมื่อเทียบกับจำนวนจุดอ่อนในรายการซีวีอี

จากการพิจารณาข้อมูลจุดอ่อนพบว่าจุดอ่อนบางรายการสามารถเกิดขึ้นได้กับเซิร์ฟเวอร์มากกว่า 1 ชนิด โดยมีคุณสมบัติต่างๆร่วมกัน ไม่ว่าจะเป็นประเภทจุดอ่อน ตำแหน่งที่เกิดจุดอ่อน ลักษณะความเสียหาย ลักษณะการโจมตี ระดับความรุนแรง และระบบปฏิบัติการที่ได้รับผลกระทบจากจุดอ่อนนั้น ซึ่งหากแยกวิเคราะห์จุดอ่อนที่เกิดขึ้นบนแต่ละเซิร์ฟเวอร์แล้วผลรวมจำนวนจุดอ่อนที่ได้ของแต่ละประเภทเซิร์ฟเวอร์รวมกันจึงเท่ากับ 1,276 รายการ แต่ถ้าวิเคราะห์จุดอ่อนของเซิร์ฟเวอร์โดยไม่แยกประเภทของเซิร์ฟเวอร์ หากจุดอ่อนใดสามารถเกิดขึ้นได้มากกว่า 1 เซิร์ฟเวอร์ก็จะนับว่าจุดอ่อนที่เกิดขึ้นนั้นเป็นจุดอ่อนเพียงรายการเดียวเท่านั้น ซึ่ง 1 รายการนี้ก็คือ 1 หมายเลขซีวีอี ดังนั้นจุดอ่อนทั้งหมดของเซิร์ฟเวอร์ที่ไม่มีการแยกประเภทจึงมีเพียง 1,252 รายการ เท่านั้น ซึ่งเมื่อนำข้อมูลที่ได้จากตาราง 5.1-5.6 มาสร้างและแสดงผลในรูปแบบของกราฟ สามารถประเมินผลลัพธ์ที่ได้ ดังต่อนี้

5.2 การประเมินและเปรียบเทียบจุดอ่อนและความเปราะบางต่อการโจมตีบนเซิร์ฟเวอร์

เนื่องจากข้อมูลที่มีอยู่หลายมิติทำให้การวิเคราะห์ ประเมินและเปรียบเทียบจุดอ่อนและความเปราะบางสามารถทำได้ในหลายมุมมองมากมาย ซึ่งคงไม่สามารถวิเคราะห์และเปรียบเทียบทุกมุมมองได้หมดในงานวิจัยนี้ ดังนั้นงานวิจัยนี้จึงยกตัวอย่างการวิเคราะห์เปรียบเทียบจุดอ่อนและความเปราะบางบนเซิร์ฟเวอร์ในมุมมองที่น่าสนใจเพียงบางมุมมองเท่านั้นดังต่อไปนี้

5.2.1 ประเมินและเปรียบเทียบจุดอ่อนที่เกิดขึ้นกับเซิร์ฟเวอร์ประเภทต่าง ๆ

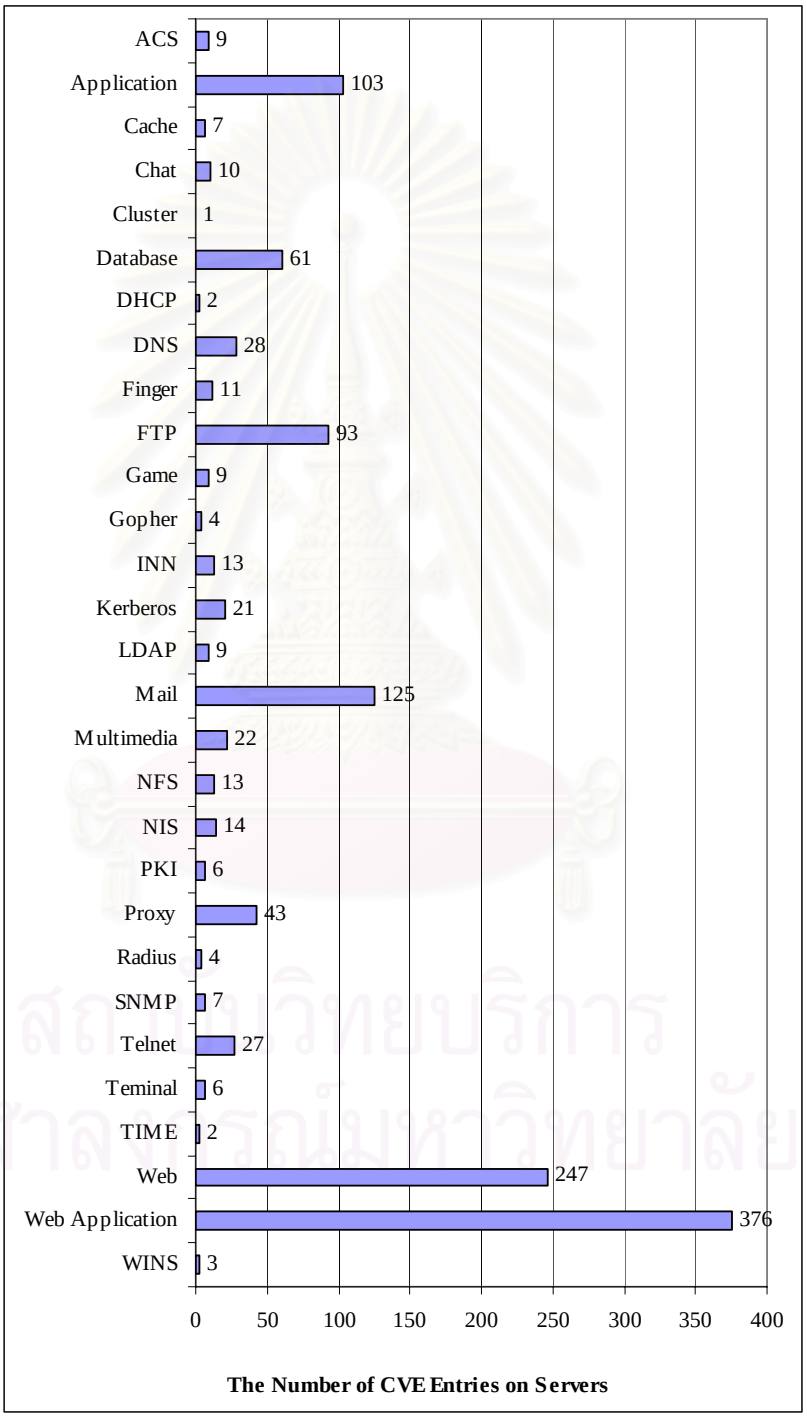
จุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์นั้นมีมากน้อยต่างกันไปขึ้นอยู่กับประเภทของเซิร์ฟเวอร์ เมื่อนำข้อมูลจำนวนจุดอ่อนที่ได้มาสร้างเป็นกราฟโดยเรียงตามจำนวนจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์ จะได้ว่าเซิร์ฟเวอร์ที่จัดอยู่ในกลุ่มที่เป็นที่นิยมหรือมีการใช้งานจากผู้ใช้จำนวนมากและสามารถเข้าถึงผ่านทางอินเทอร์เน็ตได้โดยง่ายและกว้างขวางจะมีจำนวนจุดอ่อนมากกว่าเซิร์ฟเวอร์ประเภทอื่นๆ ดังแสดงในรูปที่ 5.4 และ 5.5 เซิร์ฟเวอร์ที่พบว่ามีจำนวนจุดอ่อนเป็นจำนวนมาก ได้แก่ เว็บแอพพลิเคชั่นเซิร์ฟเวอร์ (Web Application Server), เว็บเซิร์ฟเวอร์ (Web Server), เมล์เซิร์ฟเวอร์ (Mail Server), แอพพลิเคชั่นเซิร์ฟเวอร์ (Application Server), เอฟทีพีเซิร์ฟเวอร์ (FTP Server), ดาต้าเบสเซิร์ฟเวอร์ (Database Server), พรอกซี่เซิร์ฟเวอร์ (Proxy Server) ส่วนเซิร์ฟเวอร์ที่พบจำนวนจุดอ่อนเป็นจำนวนน้อย ได้แก่ วินส์เซิร์ฟเวอร์ (WINS Server), ดีเอชซีพีเซิร์ฟเวอร์ (DHCP Server), ไทม์เซิร์ฟเวอร์ (Time Server), คลัสเตอร์เซิร์ฟเวอร์ (Cluster Server)

ในการประเมินและเปรียบเทียบจุดอ่อนที่เกิดขึ้นกับเซิร์ฟเวอร์ประเภทต่างๆนี้ จะเปรียบเทียบจุดอ่อนที่เกิดขึ้นโดยเรียงตามประเภทของจุดอ่อน จุดที่เกิดจุดอ่อน ลักษณะความเสียหายที่เกิดขึ้นตามลำดับ โดยแสดงในรูปแบบของกราฟซึ่งประกอบไปด้วยกราฟต่างๆดังต่อไปนี้

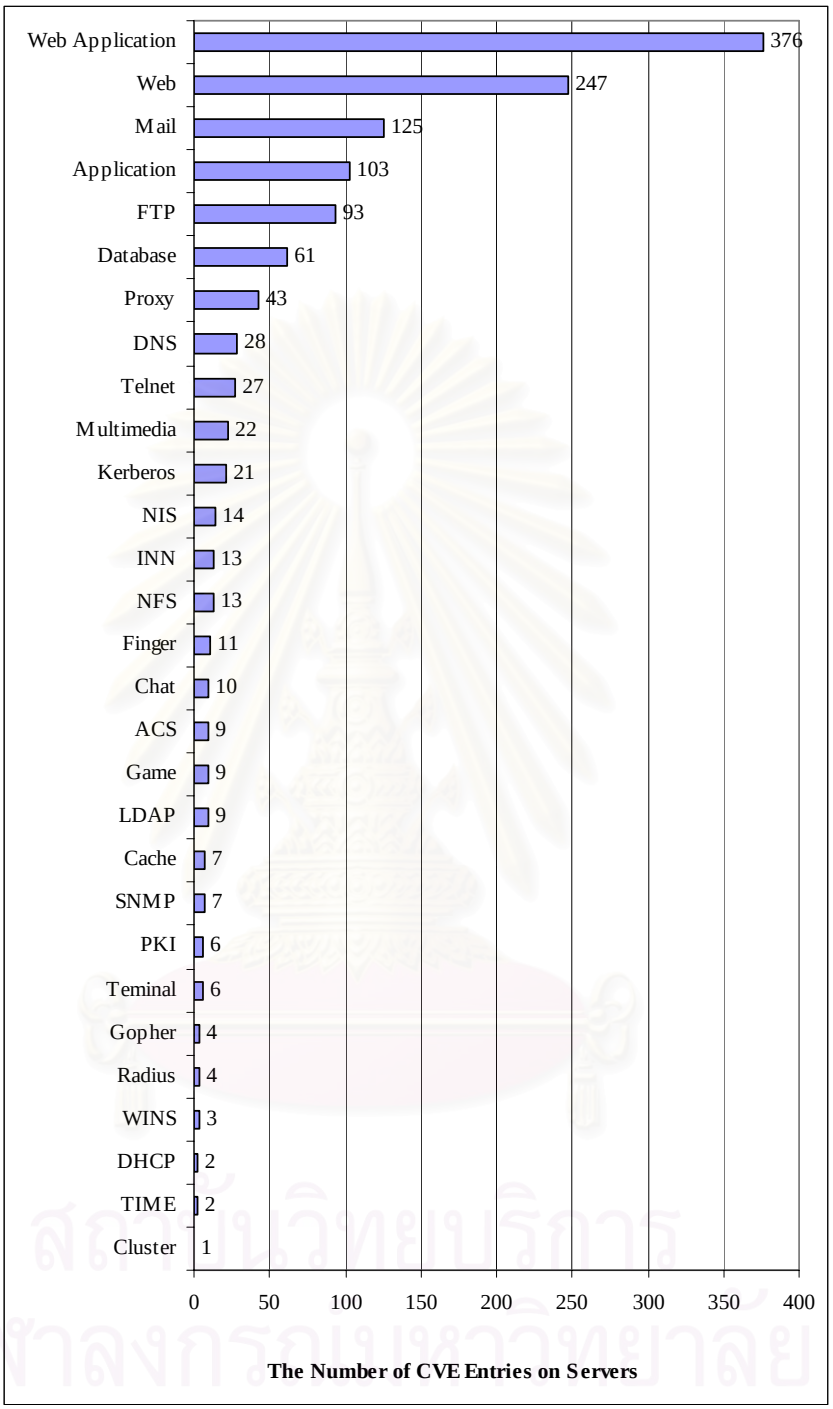
1. กราฟแสดงจำนวนรายการจุดอ่อนบนเซิร์ฟเวอร์แต่ละประเภทเรียงตามชื่อของเซิร์ฟเวอร์ (รูปที่ 5.4)
2. กราฟแสดงจำนวนรายการจุดอ่อนบนเซิร์ฟเวอร์แต่ละประเภทเรียงตามจำนวนจุดอ่อน (รูปที่ 5.5)
3. กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์แยกตามประเภทจุดอ่อนและปีที่เกิดจุดอ่อน (ในรูปที่ 5.6)
4. กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์แยกตามประเภทจุดอ่อน (รูปที่ 5.7)
5. กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์แยกตามจุดที่เกิดจุดอ่อนและปีที่เกิดจุดอ่อน (รูปที่ 5.8)
6. กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์แยกตามจุดที่เกิดจุดอ่อน (รูปที่ 5.9)

7. กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์แยกตามลักษณะความเสียหายและปีที่เกิดจุดอ่อน (รูปที่ 5.10)

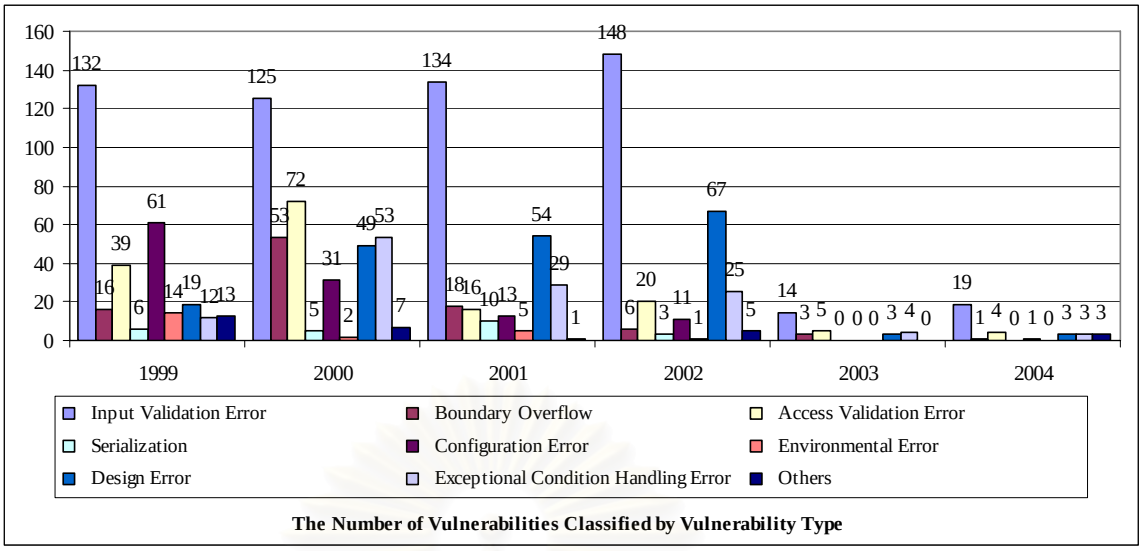
8. กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์แยกตามลักษณะความเสียหาย (รูปที่ 5.11)



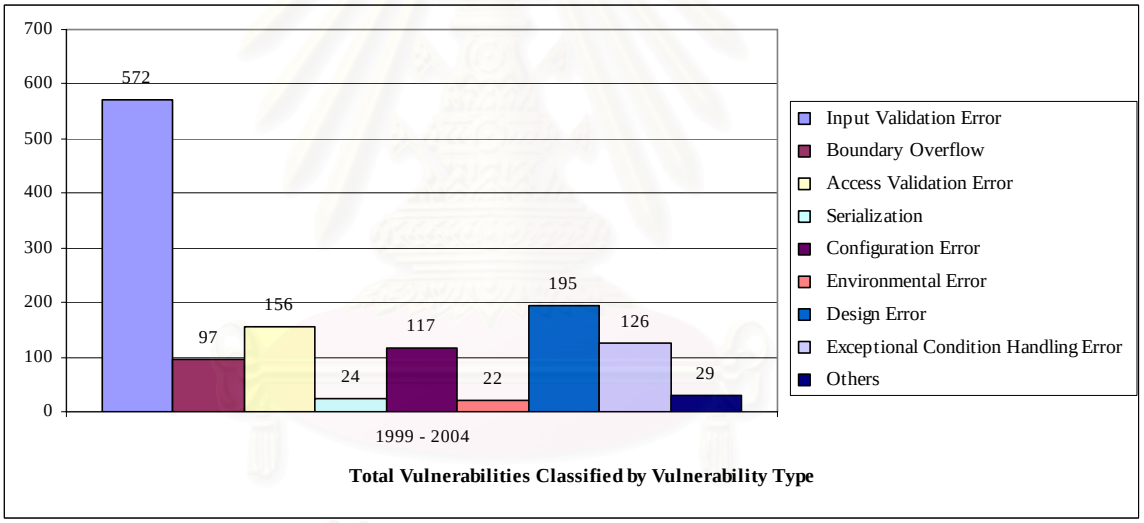
รูปที่ 5.4 กราฟแสดงจำนวนรายการจุดอ่อนบนเซิร์ฟเวอร์แต่ละประเภทเรียงตามชื่อของเซิร์ฟเวอร์



รูปที่ 5.5 **กราฟแสดงจำนวนรายการจุดอ่อนบนเซิร์ฟเวอร์แต่ละประเภทเรียงตามจำนวนจุดอ่อน**

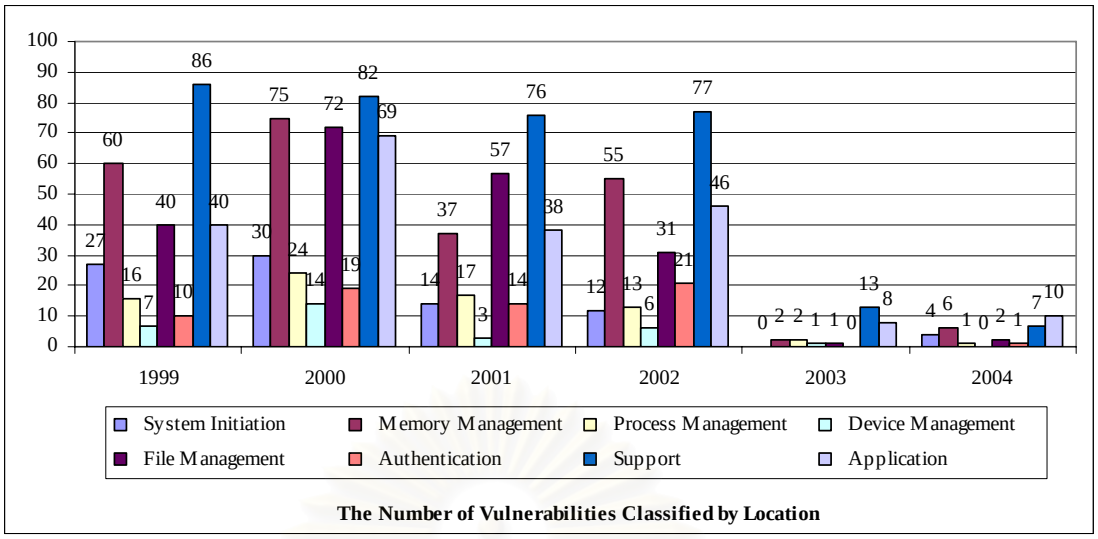


รูปที่ 5.6 กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์แยกตามประเภทจุดอ่อนและปีที่เกิดจุดอ่อน

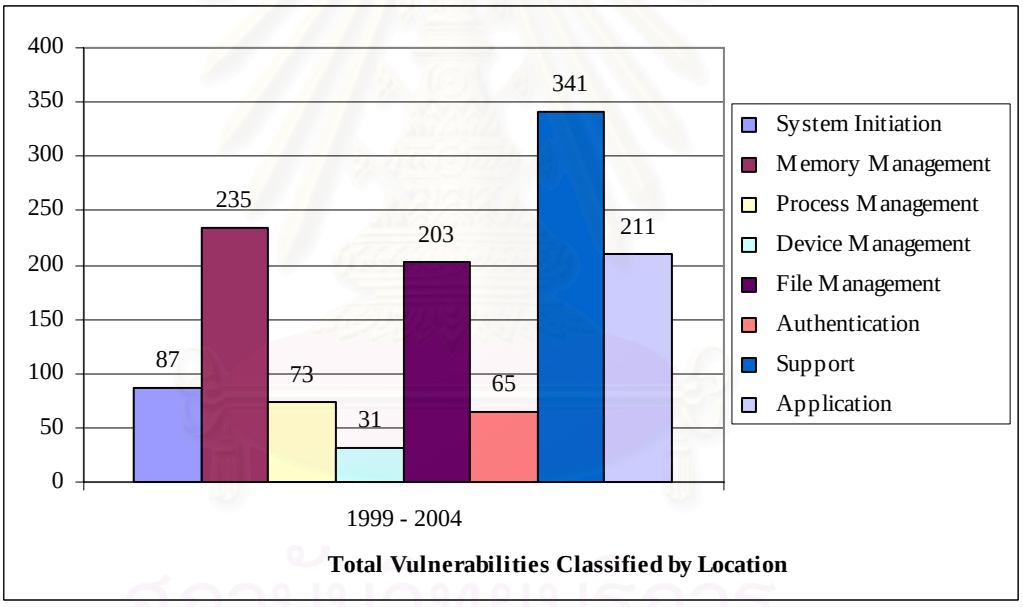


รูปที่ 5.7 กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์แยกตามประเภทจุดอ่อน

จากรูปที่ 5.6 – 5.7 แสดงถึงจุดอ่อนประเภทต่างๆที่พบบนเซิร์ฟเวอร์ ซึ่งเมื่อพิจารณาจากภาพรวมจุดอ่อนที่เกิดขึ้นพบว่าจุดอ่อนที่ถูกพบมากที่สุด ได้แก่ จุดอ่อนที่เกิดจากความผิดพลาดของการตรวจสอบข้อมูลนำเข้า ซึ่งมีจำนวนคิดเป็นร้อยละ 42.75 ของประเภทจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์ทั้งหมด การตรวจสอบข้อมูลนำเข้าดูเป็นปัญหาไม่ใหญ่มากนักและน่าที่จะสามารถป้องกันได้ แต่กลับเป็นช่องโหว่ที่สำคัญที่มักถูกนำมาใช้ในการโจมตีต่อเซิร์ฟเวอร์ ซึ่งทางผู้พัฒนาซอฟต์แวร์อาจจะมองข้ามปัญหาข้อนี้ไป หรือไม่ได้ให้ความสำคัญในการตรวจสอบข้อมูลนำเข้าเท่าที่ควรเพื่อลดความยุ่งยากซับซ้อนในการเขียนโปรแกรม ปัญหารองลงมา คือ ความผิดพลาดจากการออกแบบระบบและประเภทของจุดอ่อนที่พบน้อยที่สุด คือความผิดพลาดจากสภาพแวดล้อม

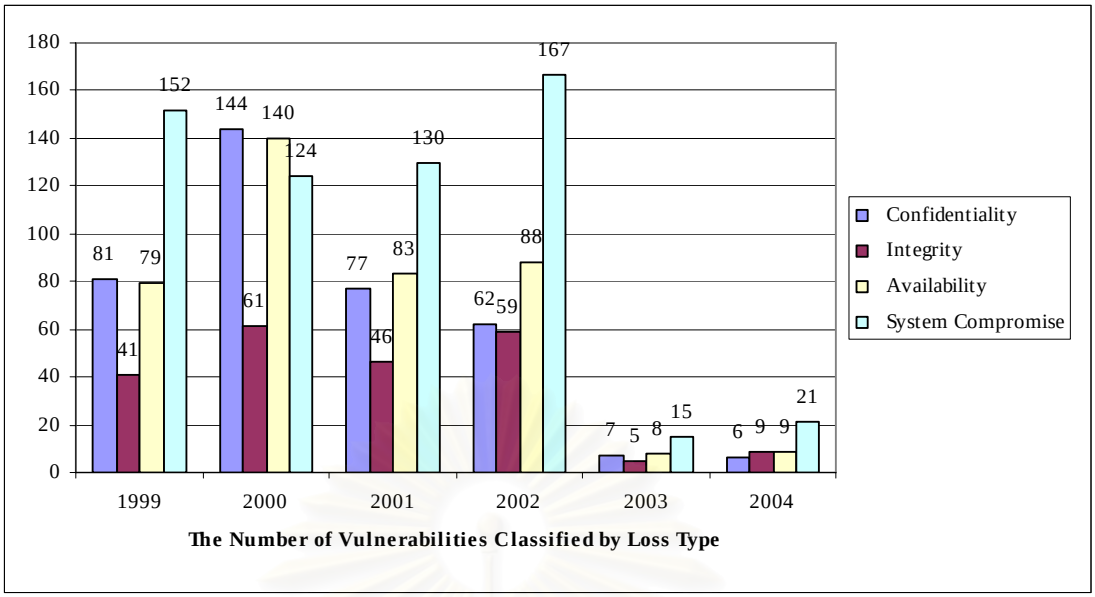


รูปที่ 5.8 กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์แยกตามจุดที่เกิดจุดอ่อนและปีที่เกิดจุดอ่อน

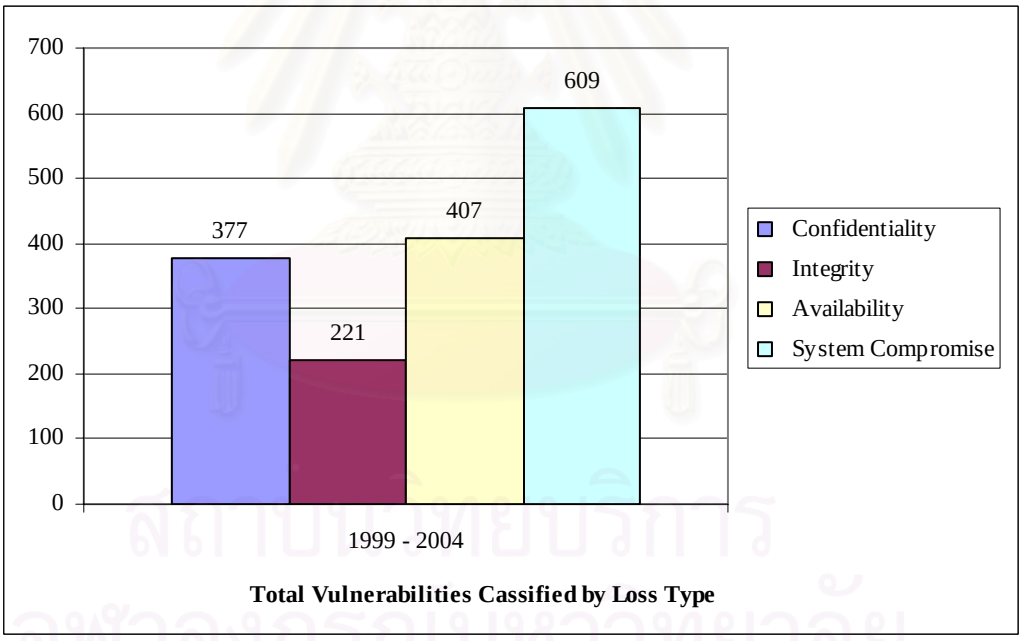


รูปที่ 5.9 กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์แยกตามจุดที่เกิดจุดอ่อน

จากรูปที่ 5.8 – 5.9 แสดงถึงจำนวนจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์โดยแยกตามจุดที่เกิดจุดอ่อน ซึ่งพบว่าจุดอ่อนส่วนมากมักจะเกิดกับส่วนของซอฟต์แวร์ที่ทำหน้าที่สนับสนุนการทำงานของระบบปฏิบัติการ เช่น ระบบจัดการฐานข้อมูล ซึ่งซอฟต์แวร์พวกนี้มักจะได้รับเอกสิทธิ์ (Privilege) บางประการจากระบบปฏิบัติการ จุดที่เกิดจุดอ่อนรองลงมา มักเกิดขึ้นกับการจัดการหน่วยความจำ การจัดการแฟ้มข้อมูล โปรแกรมประยุกต์ การเริ่มต้นระบบ การจัดการการประมวลผล การพิสูจน์ตัวจริง และการจัดการอุปกรณ์ ตามลำดับ



รูปที่ 5.10 กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์แยกตามลักษณะความเสียหายและปีที่เกิดจุดอ่อน



รูปที่ 5.11 กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์แยกตามลักษณะความเสียหาย

จากรูปที่ 5.10 – 5.11 แสดงถึงจำนวนจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์โดยแยกตามลักษณะความเสียหาย ซึ่งถ้าดูลักษณะความเสียหายที่เกิดขึ้นแล้วความเสียหายในลักษณะที่ระบบถูกล่วงละเมิดเป็นความเสียหายที่ถูกพบมากที่สุดและน่าจะก่อให้เกิดความเสียหายที่ร้ายแรงมากที่สุดเช่นกัน ซึ่งอาจเกิดจากการเรียกใช้ชุดคำสั่งใดๆ การเพิ่มสิทธิในการทำงาน การ

เข้าถึงบัญชีผู้ใช้ หรือการเข้าถึงระดับราก รองลงมา คือ การเสียสภาพพร้อมใช้งาน การเสียความเป็นความลับและการเสียบูรณะภาพ

5.2.2 ประเมินและเปรียบเทียบความเปราะบางต่อการโจมตีของเซิร์ฟเวอร์ประเภทต่าง ๆ

การสร้างกราฟเพื่อวิเคราะห์และเปรียบเทียบข้อมูลจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์ในหัวข้อ 5.1 ทำให้ทราบว่าเซิร์ฟเวอร์ประเภทใดมีจุดอ่อนมากน้อยกว่ากัน ทั้งนี้เมื่อมองในภาพรวมของเซิร์ฟเวอร์ทั้งหมดทำเห็นได้ว่า จุดอ่อนที่เกิดขึ้นส่วนใหญ่นั้นมักเกิดขึ้นในลักษณะใดและมักเกิดขึ้นที่ใดเป็นเป็นหลัก แต่เนื่องจากแต่ละจุดอ่อนที่เกิดขึ้นแต่ละจุดอ่อนมีระดับความเสียหายที่แตกต่างกัน ระดับความเสียหายที่สูงกว่าย่อมทำให้ส่งผลอันตรายร้ายแรงกว่า เมื่อคำนวณคะแนนความเปราะบางของเซิร์ฟเวอร์จากความเสียหายที่เกิดขึ้น และนำผลที่ได้มาสร้างกราฟเพื่อเปรียบเทียบในลักษณะเช่นเดียวกับการวิเคราะห์จุดอ่อนในหัวข้อ 5.1 ผลที่ได้ทำให้ทราบว่าความเปราะบางของเซิร์ฟเวอร์ไม่ขึ้นอยู่กับจำนวนจุดอ่อนที่เกิดขึ้นเสมอไป เซิร์ฟเวอร์ที่มีความเปราะบางจากการโจมตีสูง ย่อมก่อให้เกิดความเสียหายได้สูงเช่นเดียวกันหากโดนโจมตีจากผู้ไม่หวังดีต่อระบบ ถึงแม้ว่าความเสียหายที่เกิดขึ้นนั้นอาจจะเกิดจากจำนวนจุดอ่อนที่น้อยกว่าเซิร์ฟเวอร์อื่นๆก็ตาม ในรูปที่ 5.12 และ 5.13 จะเป็นกราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์ โดยในรูป 5.12 จะเรียงตามชื่อของเซิร์ฟเวอร์และรูปที่ 5.13 จะเรียงตามคะแนนความเปราะบางที่เกิดขึ้น

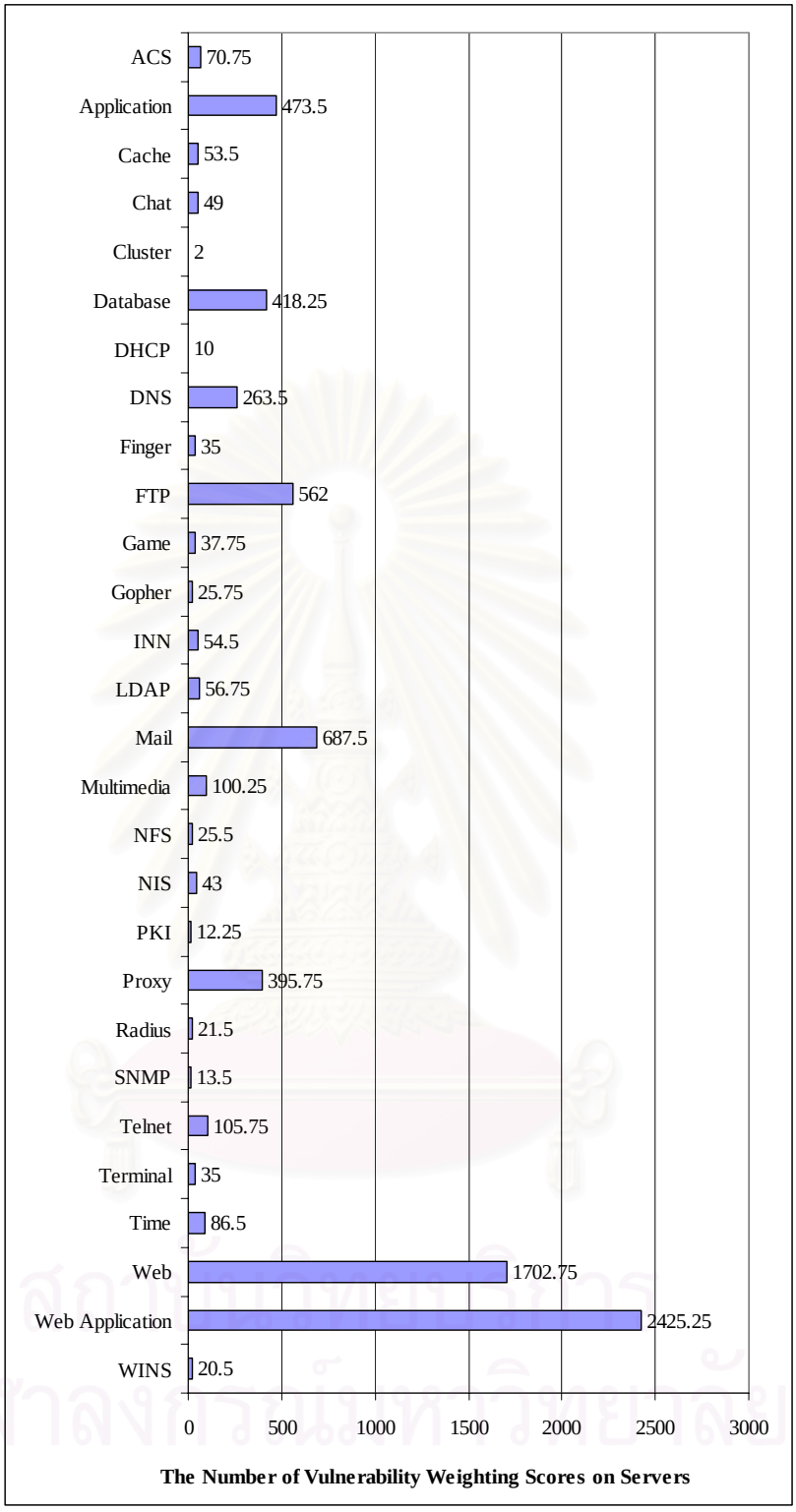
ลำดับที่	เซิร์ฟเวอร์ที่มีจุดอ่อนมากที่สุด	เซิร์ฟเวอร์ที่มีคะแนนความเปราะบางมากที่สุด
1	เว็บแอพพลิเคชั่นเซิร์ฟเวอร์	เว็บแอพพลิเคชั่นเซิร์ฟเวอร์
2	เว็บเซิร์ฟเวอร์	เว็บเซิร์ฟเวอร์
3	เมล์เซิร์ฟเวอร์	เมล์เซิร์ฟเวอร์
4	แอพพลิเคชั่นเซิร์ฟเวอร์	เอฟทีพีเซิร์ฟเวอร์
5	เอฟทีพีเซิร์ฟเวอร์	แอพพลิเคชั่นเซิร์ฟเวอร์

ตารางที่ 5.7 แสดงรายชื่อเซิร์ฟเวอร์ที่มีจุดอ่อนและคะแนนความเปราะบางมากที่สุด 5 อันดับแรก

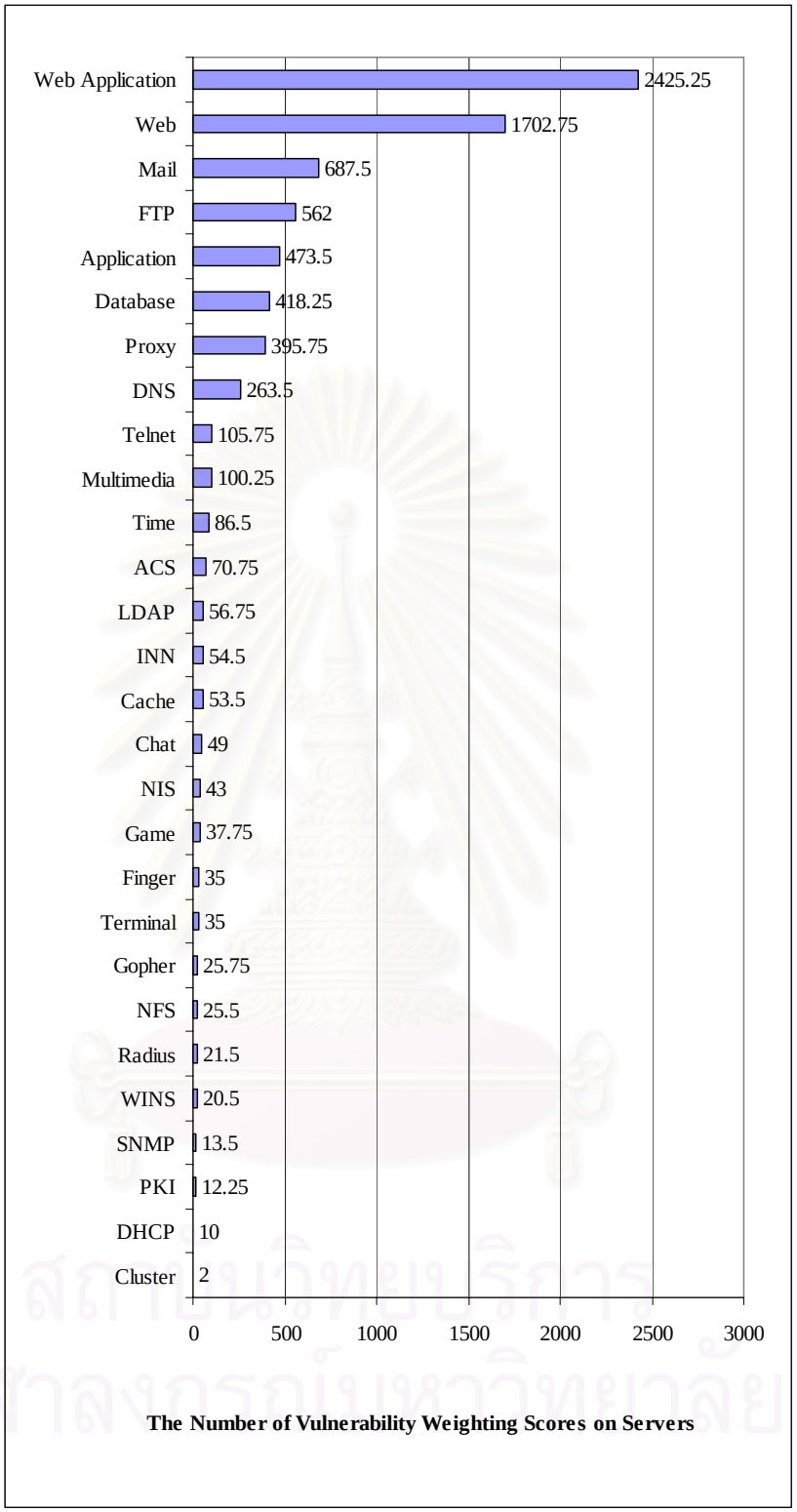
จากตาราง 5.7 แอพพลิเคชั่นเซิร์ฟเวอร์มีจุดอ่อน 103 จุด ในขณะที่เอฟทีพีเซิร์ฟเวอร์มีจุดอ่อนเพียง 93 จุด แต่หากวัดความเปราะบางต่อการโจมตี เอฟทีพีเซิร์ฟเวอร์มีความเปราะบางมากกว่าแอพพลิเคชั่นเซิร์ฟเวอร์ โดยมีคะแนนถึง 562 คะแนน ต่างจากแอพพลิเคชั่นเซิร์ฟเวอร์ที่มีคะแนนความเปราะบางเพียง 473.5 คะแนน ซึ่งยืนยันได้ว่าเซิร์ฟเวอร์ที่มีจำนวนจุดอ่อนน้อยกว่าอาจมีความเปราะบางต่อการโจมตีมากกว่าเซิร์ฟเวอร์ที่มีจำนวนจุดอ่อนที่มากกว่าได้ และหากโดนโจมตีก็อาจจะก่อให้เกิดความเสียหายขึ้นได้มากกว่าเช่นกัน

ในการประเมินและเปรียบเทียบความเปราะบางต่อการโจมตีของเซิร์ฟเวอร์ประเภทต่างๆนี้ จะเปรียบเทียบความเปราะบางของเซิร์ฟเวอร์โดยเปรียบเทียบประเภทของจุดอ่อนกับลักษณะความเสียหายที่เกิดขึ้นจากจุดอ่อนนั้น และเปรียบเทียบจุดที่เกิดจุดอ่อนกับลักษณะความเสียหายที่เกิดขึ้น โดยแสดงในรูปแบบของกราฟซึ่งประกอบไปด้วยกราฟต่างๆดังต่อไปนี้

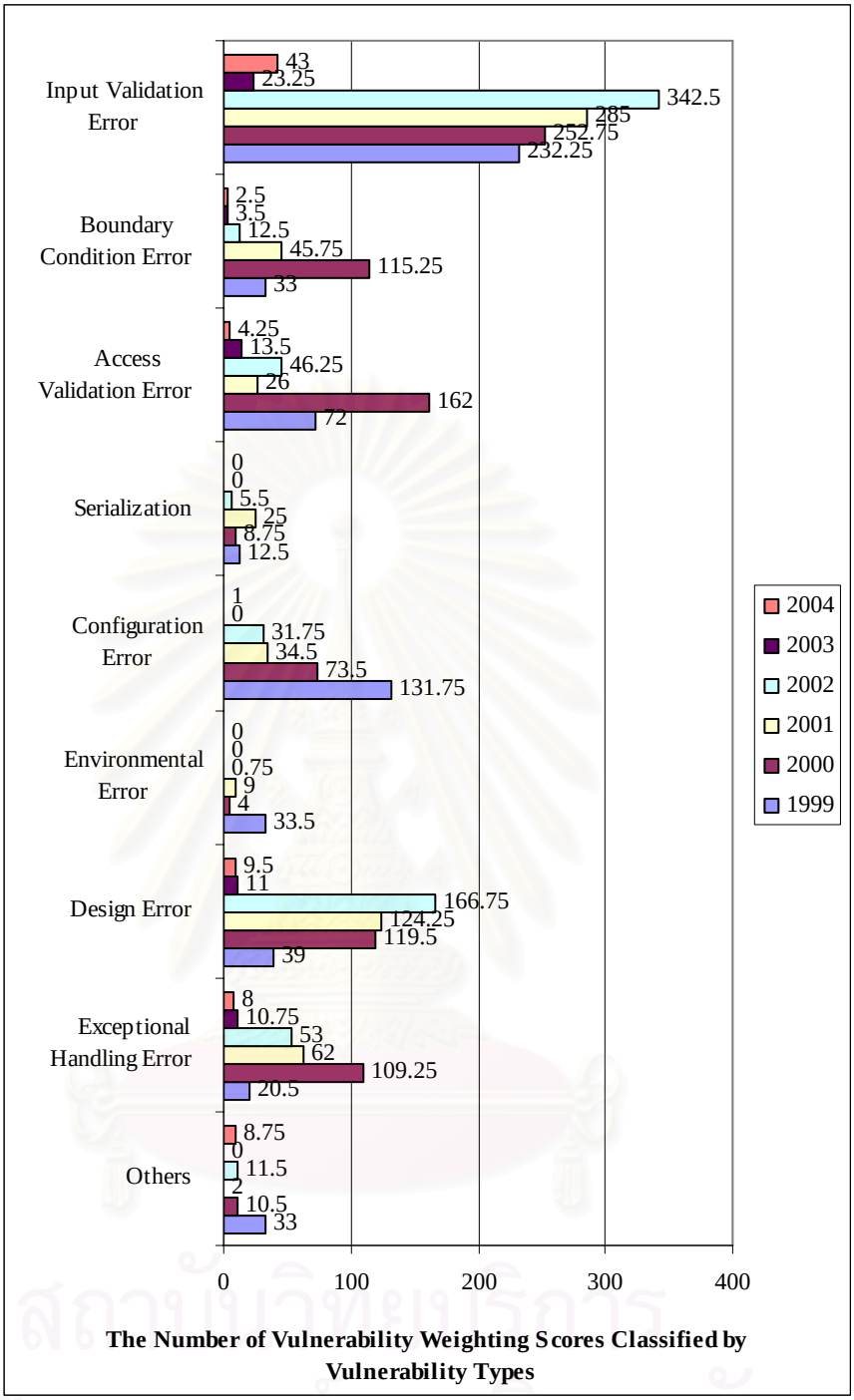
1. กราฟแสดงคะแนนความเปราะบางต่อการโจมตีบนเซิร์ฟเวอร์เรียงตามชื่อของเซิร์ฟเวอร์ (รูปที่ 5.12)
2. กราฟแสดงคะแนนความเปราะบางต่อการโจมตีบนเซิร์ฟเวอร์เรียงตามคะแนน (รูปที่ 5.13)
3. กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์แยกตามประเภทของจุดอ่อนและปีที่เกิดจุดอ่อน (รูปที่ 5.14)
4. กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์แยกตามประเภทจุดอ่อน (รูปที่ 5.15)
5. กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์แยกตามจุดที่เกิดจุดอ่อนและปีที่เกิดจุดอ่อน (รูปที่ 5.16)
6. กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์แยกตามจุดที่เกิดจุดอ่อน (รูปที่ 5.17)
7. กราฟแสดงอัตราส่วนร้อยละของความเปราะบางบนเซิร์ฟเวอร์ตามจุดที่เกิดจุดอ่อน (รูปที่ 5.18)



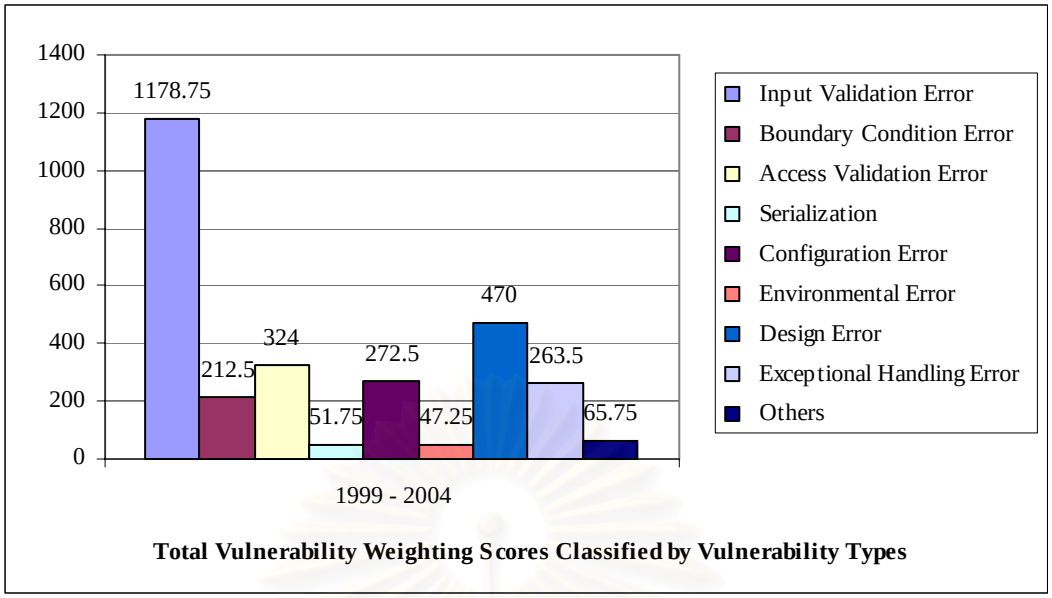
รูปที่ 5.12 **กราฟแสดงคะแนนความเปราะบางต่อการโจมตีบนเซิร์ฟเวอร์เรียงตามชื่อของเซิร์ฟเวอร์**



รูปที่ 5.13 **กราฟแสดงคะแนนความเปราะบางต่อการโจมตีบนเซิร์ฟเวอร์เรียงตามคะแนน**



รูปที่ 5.14 **กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์แยกตามประเภทของจุดอ่อนและปีที่เกิดจุดอ่อน**



รูปที่ 5.15 กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์แยกตามประเภทของจุดอ่อน

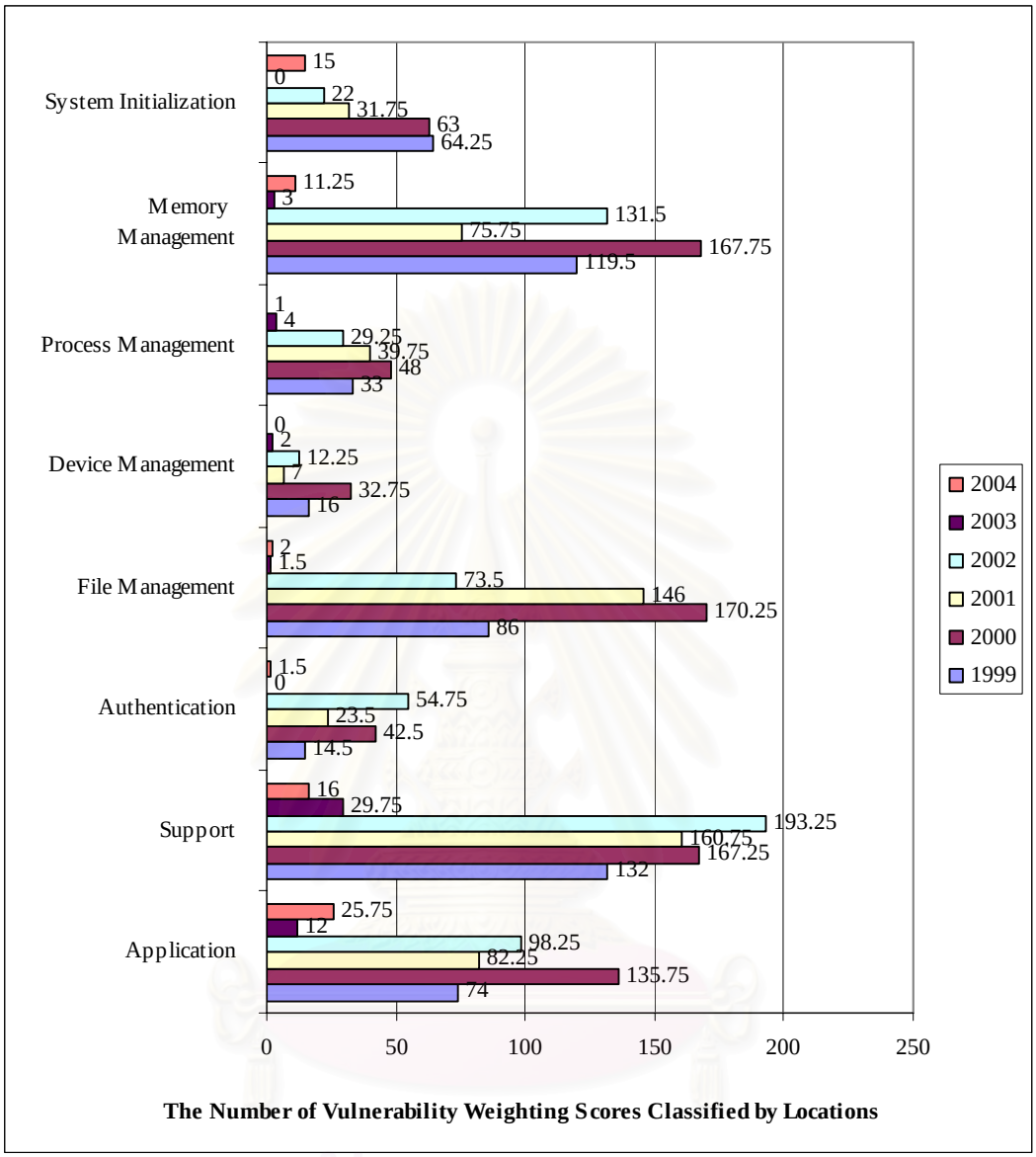
จากรูปที่ 5.14 และ 5.15 แสดงกราฟคะแนนความเปราะบางของเซิร์ฟเวอร์โดยแยกออกตามประเภทของจุดอ่อนและปีที่เกิดจุดอ่อน ผลที่ได้ คือ ความเปราะบางที่เกิดขึ้นบนเซิร์ฟเวอร์ส่วนใหญ่เกิดจากปัญหาการตรวจสอบข้อมูลนำเข้าซึ่งเป็นปัญหาที่มีคะแนนความเปราะบางสูงที่สุด การป้องกันปัญหาดังกล่าวมักทำให้การเขียนโปรแกรมต้องเพิ่มฟังก์ชั่นการตรวจสอบขึ้นมากมาย เมื่อเทียบกับการโจมตีที่สามารถทำได้โดยไม่ต้องใช้วิธีการซับซ้อนมากนัก ซึ่งหากไม่มีวิธีการป้องกันที่ดีแล้วจุดอ่อนประเภทดังกล่าวก็อาจจะก่อให้เกิดความเสียหายอย่างใหญ่หลวงได้

ในตารางที่ 5.8 จะแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์โดยแยกออกตามประเภทของจุดอ่อนที่เกิดขึ้น ซึ่งเมื่อวิเคราะห์ลงไปในรายละเอียดจะทำให้ทราบได้ว่าจุดอ่อนแต่ละประเภท สามารถก่อให้เกิดความเสียหายในรูปแบบใดมากกว่ากัน ซึ่งการผิดพลาดจากการตรวจสอบนำเข้าที่เป็นจุดเปราะบางจุดใหญ่ของเซิร์ฟเวอร์ สามารถก่อให้เกิดความเสียหายในการเสียสภาพพร้อมใช้งานมากที่สุด รองลงมาได้แก่ การถูกล่วงละเมิดยังระบบ การทำให้เสียความลับ และการเสียบูรณะภาพเป็นความเสียหายที่เกิดขึ้นจากการผิดพลาดในการตรวจสอบข้อมูลนำเข้าน้อยที่สุด

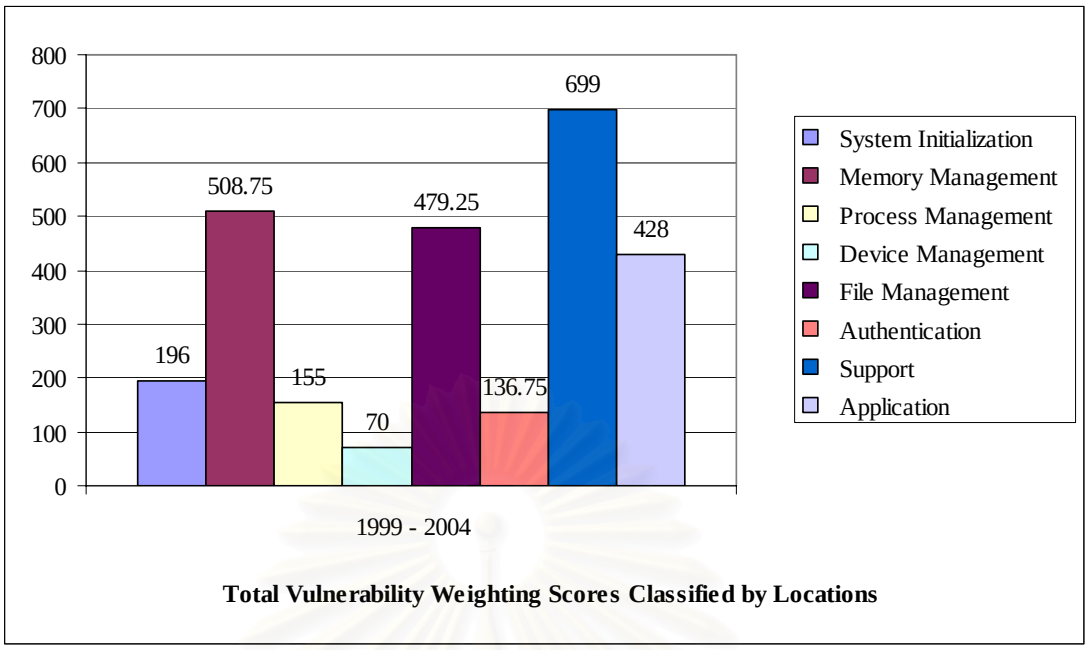
Server : All Servers : The Number of CVE Entries : 1252						
No	Vulnerability Type	Loss Type				
		1999 - 2004				
		Confidentiality	Integrity	Availability	System Compromise	Sum
1	Input Validation Error	235	181	481	281.75	1178.8
2	Boundary Condition Error	38	14	139	21.5	212.5
3	Access Validation Error	170	90	18	46	324
4	Serialization	9	18	19	5.75	51.75
5	Configuration Error	130	91	23	28.5	272.5
6	Environmental Error	16	10	16	5.25	47.25
7	Design Error	175	150	93	52	470
8	Exceptional Handling Error	50	13	186	14.5	263.5
9	Others	22	25	13	5.75	65.75
Total Number of Weighting Scores		845	592	988	461	2886

ตารางที่ 5.8 ตารางคะแนนความเปราะบางของเซิร์ฟเวอร์เมื่อเทียบประเภทของจุดอ่อนและลักษณะความเสียหายที่เกิดขึ้น

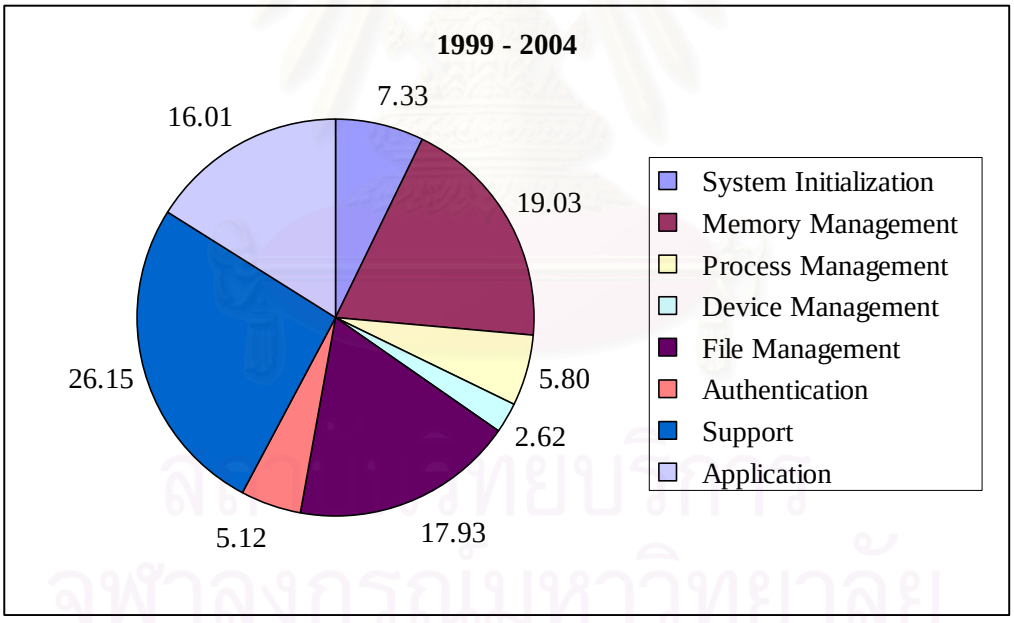
ในรูป 5.16 – 5.18 จะแสดงให้เห็นถึงความเปราะบางบนเซิร์ฟเวอร์เมื่อแยกตามจุดที่เกิดจุดอ่อน ซึ่งจากผลรวมคะแนนความเปราะบางที่ได้พบว่าจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์โดยส่วนใหญ่มักจะเกิดขึ้นกับโปรแกรมที่สนับสนุนการทำงานของเซิร์ฟเวอร์ โดยมีคะแนน 699 คะแนน คิดเป็นร้อยละ 26.15 ของจุดอ่อนที่เกิดขึ้นทั้งหมดบนเซิร์ฟเวอร์ ซึ่งหมายความว่าหากผู้ไม่หวังดีต่อระบบต้องการโจมตีระบบโดยการโจมตีมายังเซิร์ฟเวอร์ที่ให้บริการแล้ว จุดดังกล่าวเป็นจุดอ่อนที่เหมาะแก่การโจมตีมากที่สุด และสามารถสร้างความเสียหายได้มากด้วยเช่นกัน จุดที่มีเสี่ยงต่อการโจมตีมากที่สุดรองมาได้แก่ ส่วนการจัดการหน่วยความจำ ส่วนการจัดการแฟ้มข้อมูล ส่วนโปรแกรมประยุกต์ ส่วนการจัดการประมวลผล ส่วนการพิสูจน์ตัวจริง และส่วนการจัดการอุปกรณ์เป็นจุดที่พบความเปราะบางจากการโจมตีน้อยที่สุด



รูปที่ 5.16 **กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์แยกตามจุดที่เกิดจุดอ่อน และปีที่เกิดจุดอ่อน**



รูปที่ 5.17 **กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์แยกตามจุดที่เกิดจุดอ่อน**



รูปที่ 5.18 **กราฟแสดงอัตราส่วนร้อยละของความเปราะบางบนเซิร์ฟเวอร์ตามจุดที่เกิดจุดอ่อน**

Server : All Servers : The Number of CVE Entries : 1252						
No.	Location	Loss Type				
		1999 - 2004				
		Confidentiality	Integrity	Availability	System Compromise	Sum
1	System Initialization	74	55	38	29	196
2	Memory Management	4	12	385	107.75	508.75
3	Process Management	7	2	140	6	155
4	Device Management	7	7	52	4	70
5	File Management	307	119	28	25.25	479.25
6	Authentication	37	46	20	33.75	136.75
7	Support	180	162	215	142	699
8	Application	165	137	41	85	428
Total Number of Weighting Scores		781	540	919	432.75	2672.8

ตารางที่ 5.9 ตารางคะแนนความเปราะบางของเซิร์ฟเวอร์เมื่อเทียบจุดที่เกิดจุดอ่อนและลักษณะความเสียหายที่เกิดขึ้น

ในตารางที่ 5.9 แสดงคะแนนความเปราะบางของเซิร์ฟเวอร์ ณ จุดที่เกิดจุดอ่อนตำแหน่งต่างๆ ทำให้ทราบได้ว่าแต่ละจุดที่เกิดจุดอ่อนนั้น สามารถเกิดความเสียหายในลักษณะใดมากที่สุด ซึ่งจากข้อมูลในตารางจุดที่มีความเปราะบางมากที่สุดได้แก่ ส่วนของโปรแกรมที่สนับสนุนการทำงานของระบบปฏิบัติการ โดยความเสียหายที่สามารถเกิดขึ้นได้มากที่สุดได้แก่ การเสียสภาพพร้อมใช้งาน ซึ่งลักษณะความเสียหายดังกล่าวที่เกิดขึ้น เมื่อนำไปเทียบกับลักษณะความเสียหายที่เกิดขึ้นสูงสุดโดยการแยกวิเคราะห์ตามประเภทของจุดอ่อนในตารางที่ 5.8 แล้วพบว่าต่างก็มีความเปราะของความเสียหายในการลักษณะของการทำให้เสียสภาพพร้อมใช้งานสูงเป็นอันดับแรกเช่นกัน ดังนั้นจึงทำให้ทราบได้ว่าเซิร์ฟเวอร์ส่วนใหญ่นั้นมักมีความเปราะบางต่อการโจมตีที่ทำให้เสียสภาพพร้อมใช้งานมากที่สุด

5.2.3 ประเมินและเปรียบเทียบจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์ของระบบปฏิบัติการประเภทต่าง ๆ

การประเมินจุดอ่อนที่เกิดขึ้นในหัวข้อที่ผ่านมาจะเป็นการประเมินโดยดูที่ภาพรวมของเซิร์ฟเวอร์ทั้งหมดเป็นหลักซึ่งทำให้พอที่จะทราบได้ว่าเซิร์ฟเวอร์ที่มีให้บริการอยู่นั้น มีจุดอ่อนและความเปราะบางในเรื่องใดมากที่สุดและมักจะเกิดขึ้นในจุดไหนบ้าง ในหัวข้อนี้จะเป็นการประเมินจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์โดยพิจารณาจากระบบปฏิบัติการที่ได้รับผลกระทบจากจุดอ่อนนั้นๆ โดยระบบปฏิบัติการได้รับผลกระทบในงานวิจัยนี้จะแบ่งออกเป็น 5 กลุ่ม ได้แก่

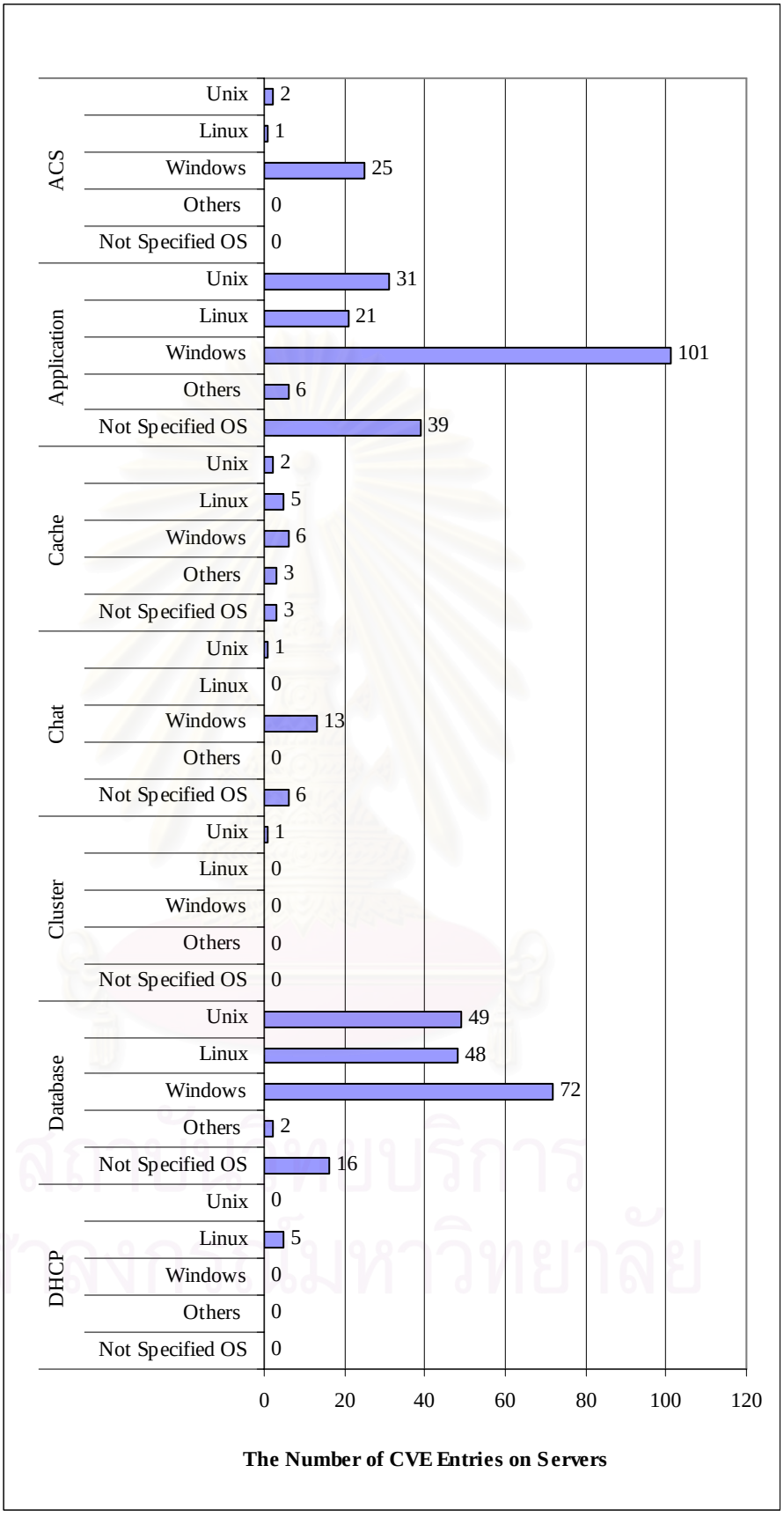
1. ระบบปฏิบัติการยูนิกซ์
2. ระบบปฏิบัติการลินุกซ์
3. ระบบปฏิบัติการวินโดวส์
4. ระบบปฏิบัติการอื่นๆ ได้แก่ โอเอสทู, เน็ตแวร์, แมคโอเอส, ซิสโก้ไอโอเอส และแคชโอเอส
5. ระบบปฏิบัติการประเภทที่ไม่มีการระบุไว้ในรายการอ้างอิง ซึ่งที่จริงแล้วระบบปฏิบัติการในกลุ่มนี้อาจเป็นระบบปฏิบัติการในกลุ่มที่ 1 – 4 กลุ่มใดกลุ่มหนึ่งหรือทั้งหมดก็ได้

ในการประเมินและเปรียบเทียบจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์ของระบบปฏิบัติการประเภทต่างๆนี้ จะเปรียบเทียบเพื่อแสดงให้เห็นว่าเซิร์ฟเวอร์ต่างๆเมื่อทำงานบนระบบปฏิบัติการใดจะก่อให้เกิดจุดอ่อนได้มากน้อยกว่ากัน โดยจะแสดงในรูปแบบของกราฟซึ่งประกอบไปด้วยกราฟต่างๆดังต่อไปนี้

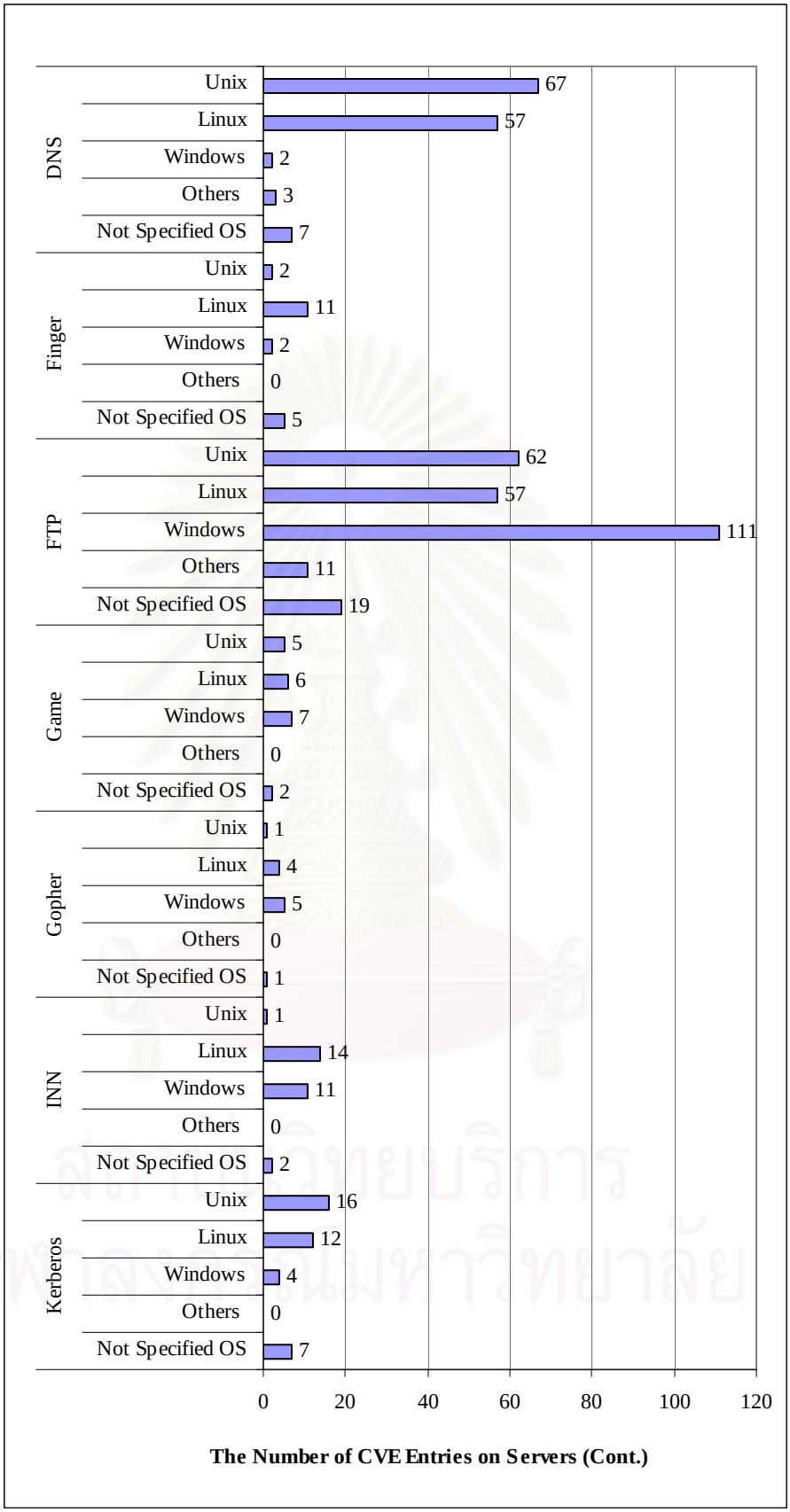
1. กราฟเปรียบเทียบจำนวนจุดอ่อนของเซิร์ฟเวอร์บนระบบปฏิบัติการต่างๆ (รูปที่ 5.19 - 5.22)
2. กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์ของระบบปฏิบัติการต่างๆ (รูปที่ 5.23)
3. กราฟแสดงอัตราส่วนร้อยละของจำนวนจุดอ่อนบนเซิร์ฟเวอร์ของระบบปฏิบัติการต่างๆ (รูปที่ 5.24)
4. กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์ของระบบปฏิบัติการยูนิกซ์ (รูปที่ 5.25)

5. กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์ของระบบปฏิบัติการลินุกซ์ (รูปที่ 5.26)
6. กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์ของระบบปฏิบัติการวินโดวส์ (รูปที่ 5.27)
7. กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์ของระบบปฏิบัติการอื่นๆและที่ไม่มีการระบุไว้ในรายการอ้างอิง (รูปที่ 5.28)
8. กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์แยกตามประเภทของระบบปฏิบัติการยูนิกซ์และปีที่เกิดจุดอ่อน (รูปที่ 5.29)
9. กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์แยกตามประเภทของระบบปฏิบัติการลินุกซ์และปีที่เกิดจุดอ่อน (รูปที่ 5.30)
10. กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์แยกตามประเภทของระบบปฏิบัติการวินโดวส์และปีที่เกิดจุดอ่อน (รูปที่ 5.31)
11. กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์แยกตามประเภทของระบบปฏิบัติการอื่นๆและปีที่เกิดจุดอ่อน (รูปที่ 5.32)

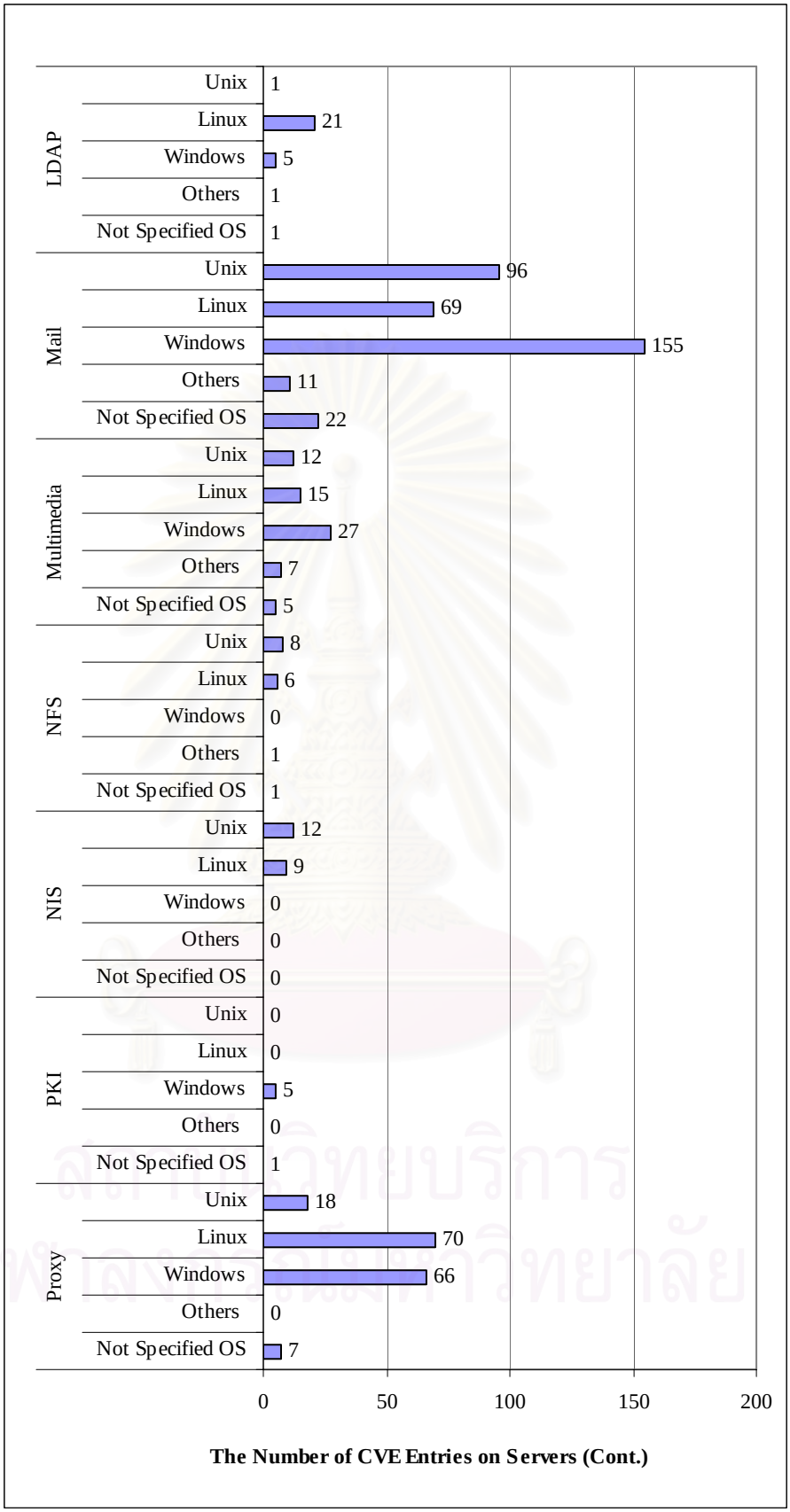
รูปที่ 5.19 – 5.22 จะเปรียบเทียบจำนวนจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์ของระบบปฏิบัติการต่างๆ โดยจะแยกให้เห็นว่าแต่ละประเภทเซิร์ฟเวอร์นั้น เมื่อทำงานบนระบบปฏิบัติการใดจะมีจำนวนจุดอ่อนที่เกิดขึ้นมากกว่ากัน



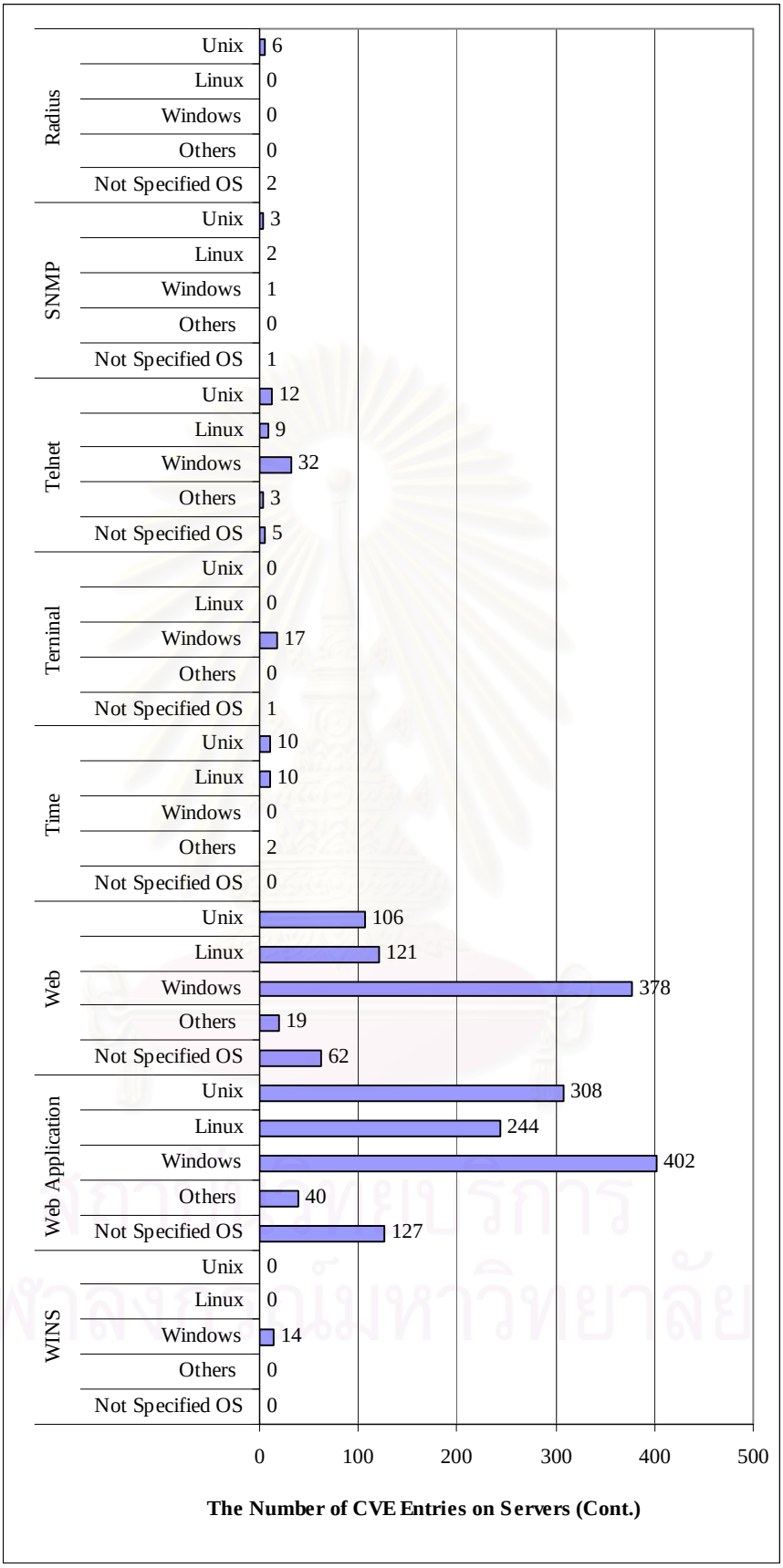
รูปที่ 5.19 **กราฟเปรียบเทียบจำนวนจุดอ่อนของเซิร์ฟเวอร์บนระบบปฏิบัติการต่าง ๆ#1**



รูปที่ 5.20 **กราฟเปรียบเทียบจำนวนจุดอ่อนของเซิร์ฟเวอร์บนระบบปฏิบัติการต่าง ๆ#2**

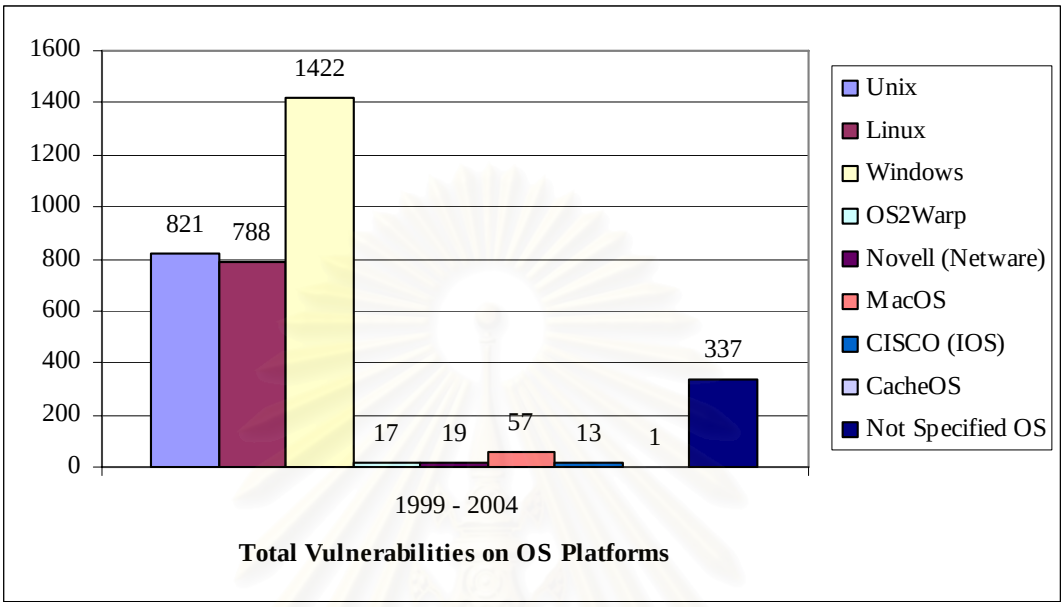


รูปที่ 5.21 กราฟเปรียบเทียบจำนวนจุดอ่อนของเซิร์ฟเวอร์บนระบบปฏิบัติการต่าง ๆ#3

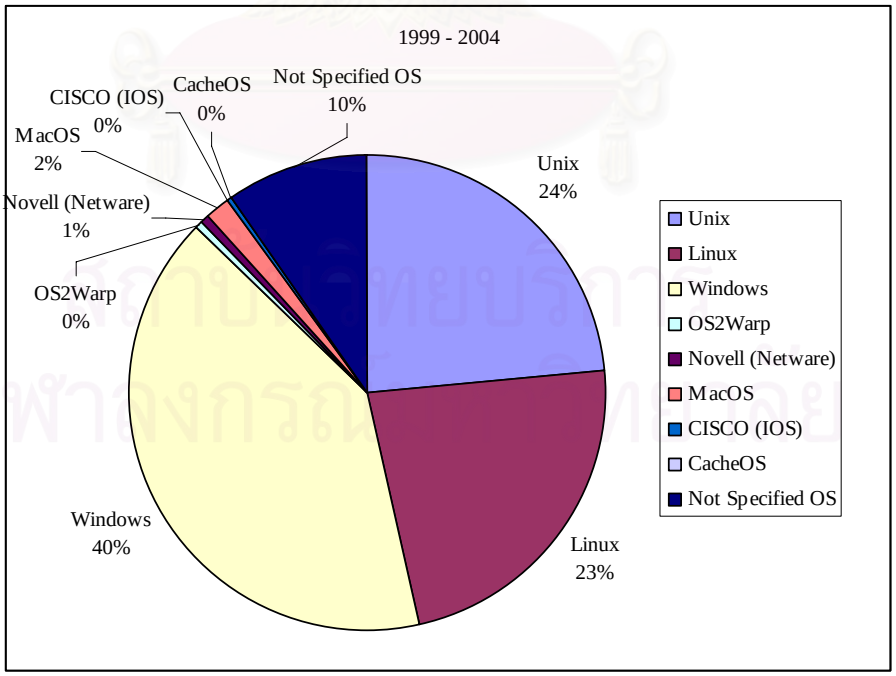


รูปที่ 5.22 กราฟเปรียบเทียบจำนวนจุดอ่อนของเซิร์ฟเวอร์บนระบบปฏิบัติการต่าง ๆ#4

เมื่อรวมจำนวนจุดอ่อนที่เกิดขึ้นกับเซิร์ฟเวอร์ทั้งหมดแล้ว พบว่าจุดอ่อนที่เกิดขึ้นนั้นมักเกิดขึ้นบนระบบปฏิบัติการวินโดวส์มากที่สุด คิดเป็นร้อยละ 40 ของจุดอ่อนทั้งหมด ดังรูปที่ 5.23 และ 5.24

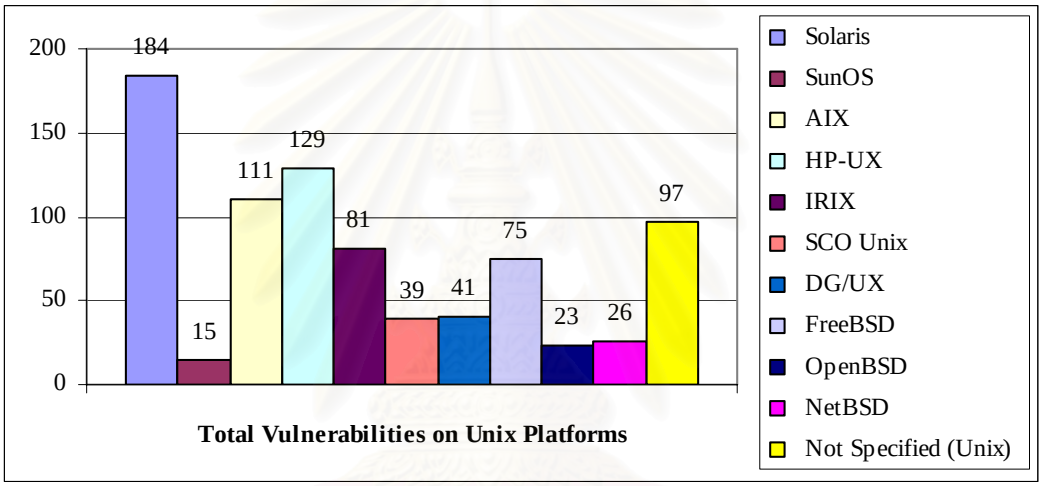


รูปที่ 5.23 กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์ของระบบปฏิบัติการต่างๆ

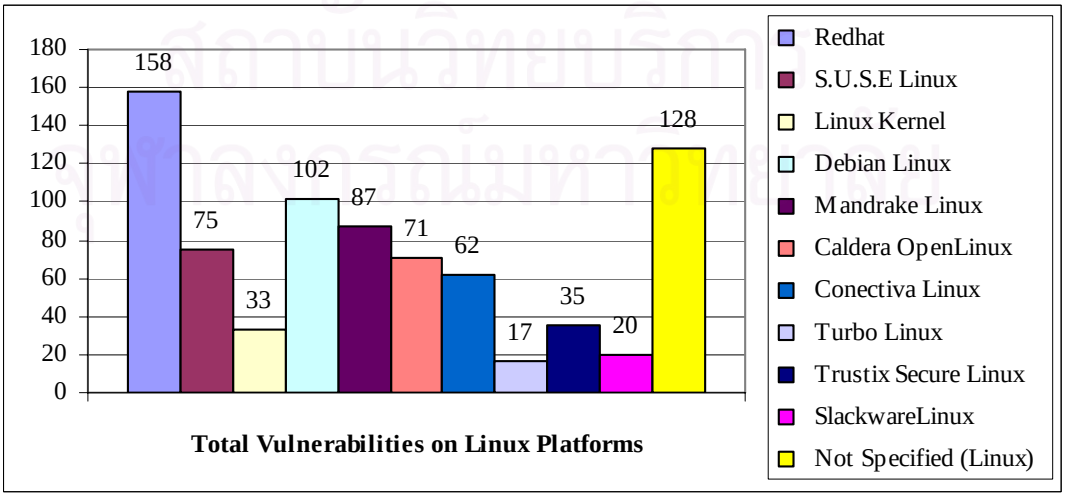


รูปที่ 5.24 กราฟแสดงอัตราส่วนร้อยละของจำนวนจุดอ่อนบนเซิร์ฟเวอร์ของระบบปฏิบัติการต่างๆ

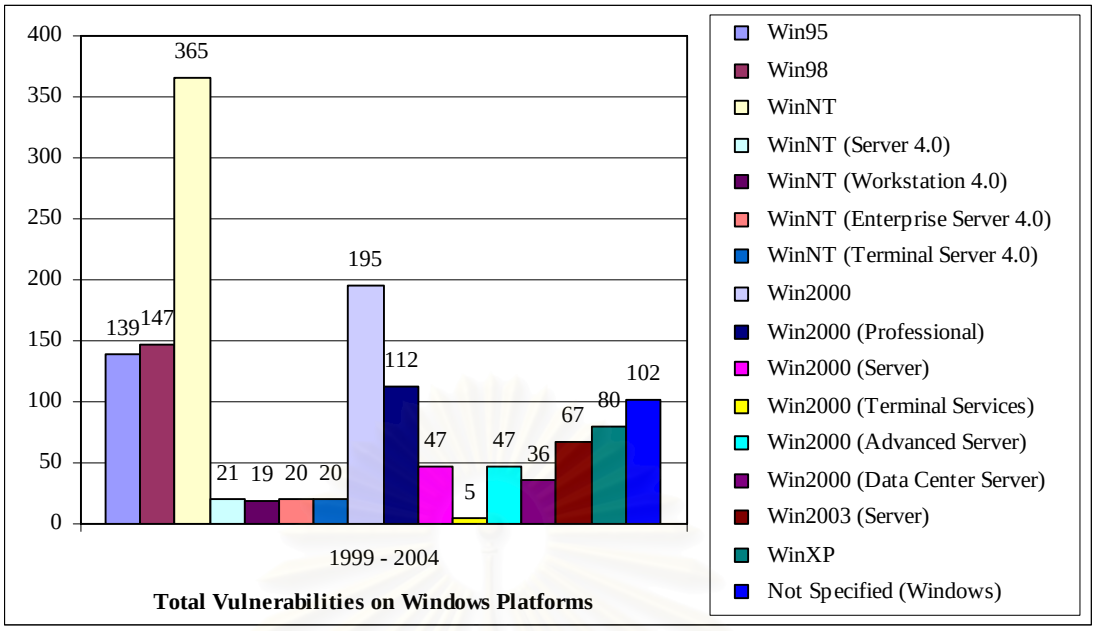
รูปที่ 5.25 – 28 แสดงจำนวนจุดอ่อนที่เกิดขึ้นบนระบบปฏิบัติการต่างๆ รูป 5.25 เป็นจุดอ่อนที่มีผลกระทบต่อระบบปฏิบัติการยูนิกซ์ซึ่งแยกจำนวนจุดอ่อนออกตามระบบปฏิบัติการยูนิกซ์ประเภทต่างๆ ซึ่งพบว่าจุดอ่อนที่เกิดขึ้นมักเกิดกับยูนิกซ์ของซันโซลาริสมากที่สุดถึง 184 จุดอ่อน รองลงมาคือ เอชพียูเอกซ์ และ เอไอเอกซ์จากไอบีเอ็ม รูปที่ 5.26 แสดงจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์ของระบบปฏิบัติการลินุกซ์ โดยเรทแฮทลินุกซ์ คือระบบปฏิบัติการแพลตฟอร์มลินุกซ์ที่มีจำนวนจุดอ่อนเกิดขึ้นมากที่สุด ในรูป 5.27 จะเป็นจุดอ่อนที่เกิดบนระบบปฏิบัติการวินโดวส์ ซึ่งถือได้ว่าเป็นระบบปฏิบัติการที่พบจุดอ่อนได้มากที่สุด ส่วนระบบปฏิบัติการวินโดวส์ที่มีจุดอ่อนมากที่สุด ได้แก่ วินโดวส์เอ็นที สุดท้าย คือรูปที่ 5.28 เป็นกราฟแสดงจุดอ่อนที่เกิดขึ้นกับระบบปฏิบัติการอื่นๆ และที่ไม่มีการระบุไว้ในรายการอ้างอิง



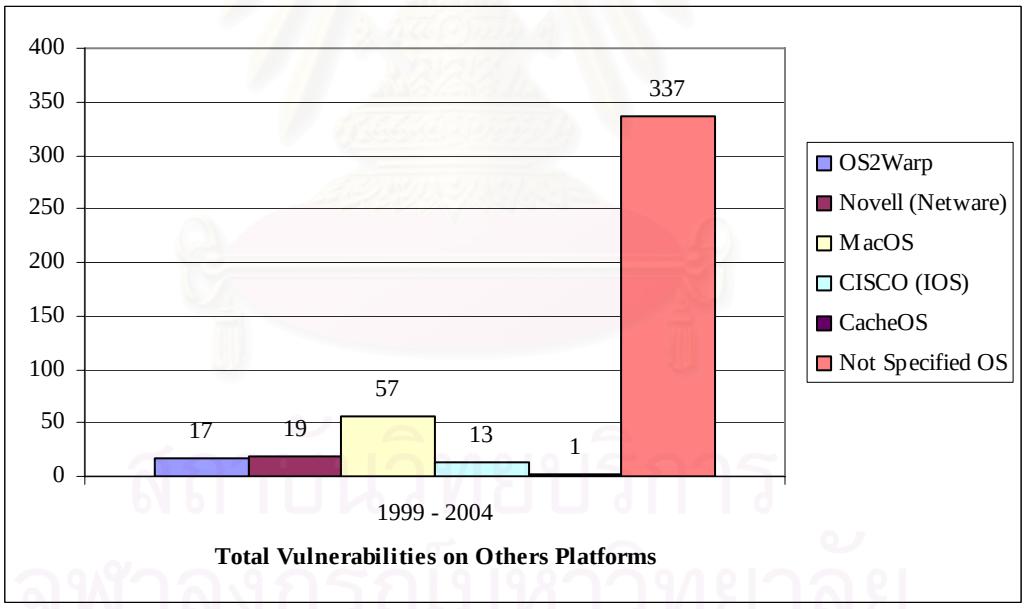
รูปที่ 5.25 กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์ของระบบปฏิบัติการยูนิกซ์



รูปที่ 5.26 กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์ของระบบปฏิบัติการลินุกซ์

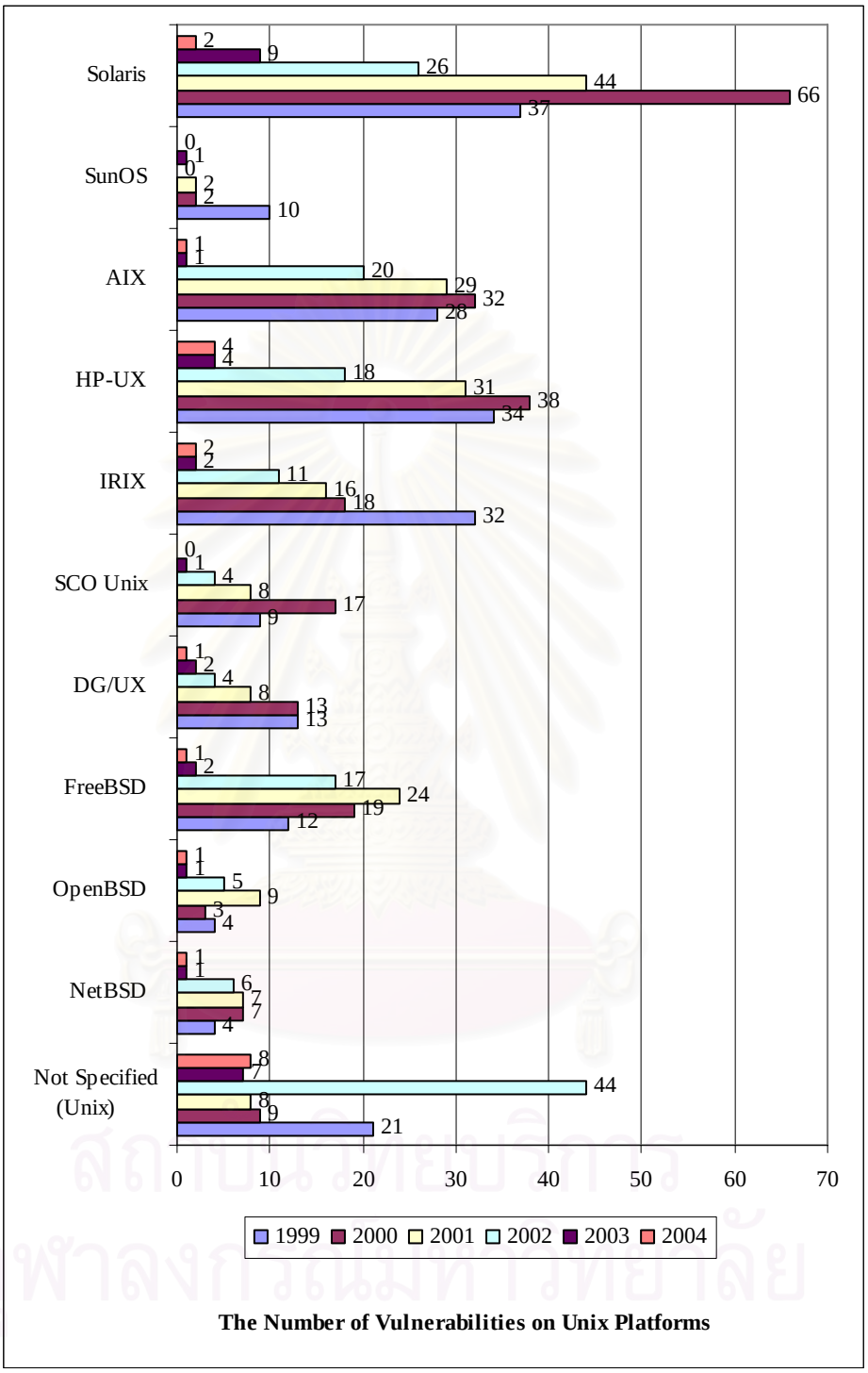


รูปที่ 5.27 กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์ของระบบปฏิบัติการวินโดวส์

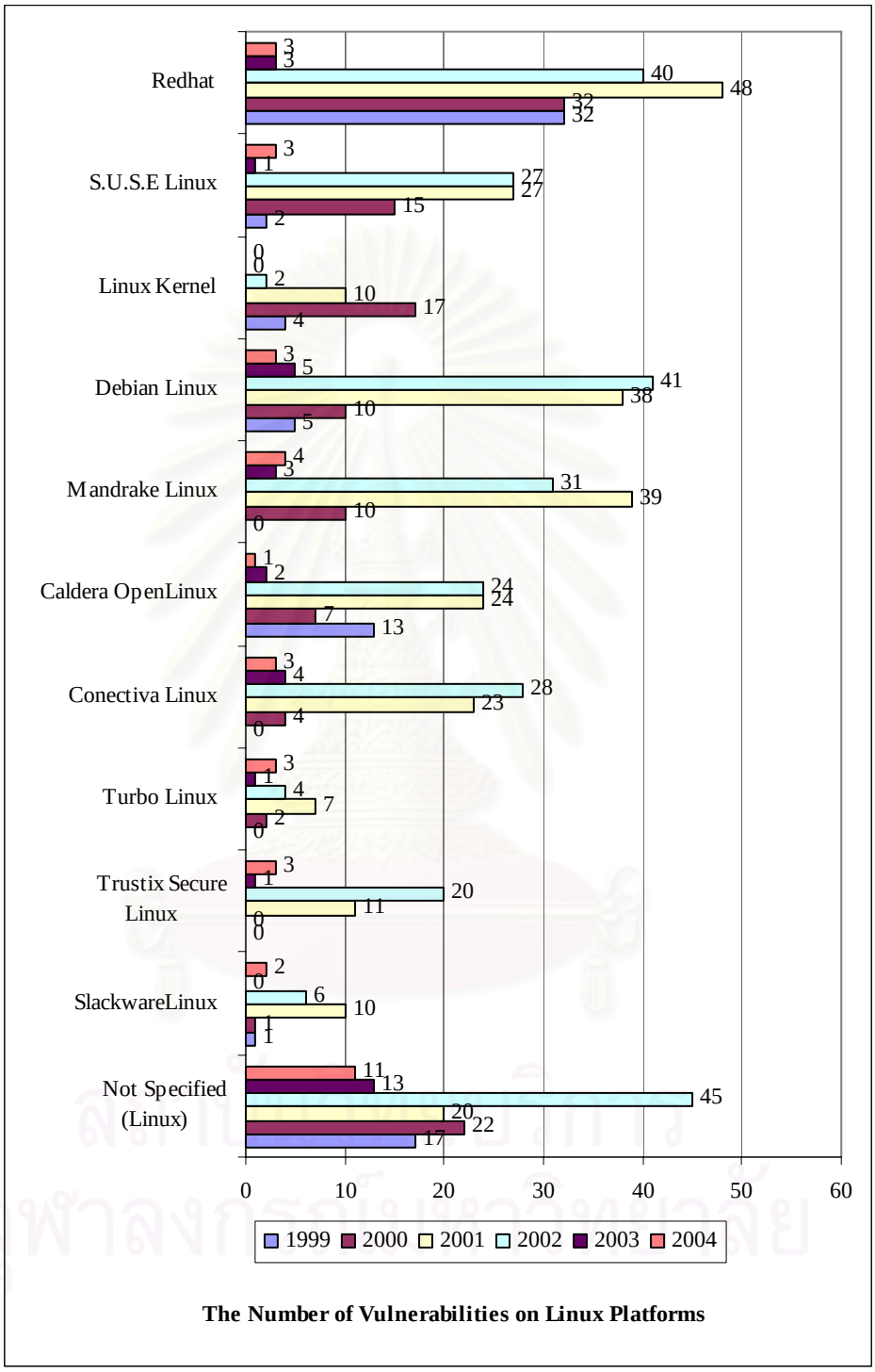


รูปที่ 5.28 กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์ของระบบปฏิบัติการอื่น ๆและที่ไม่มีการระบุไว้ในรายการอ้างอิง

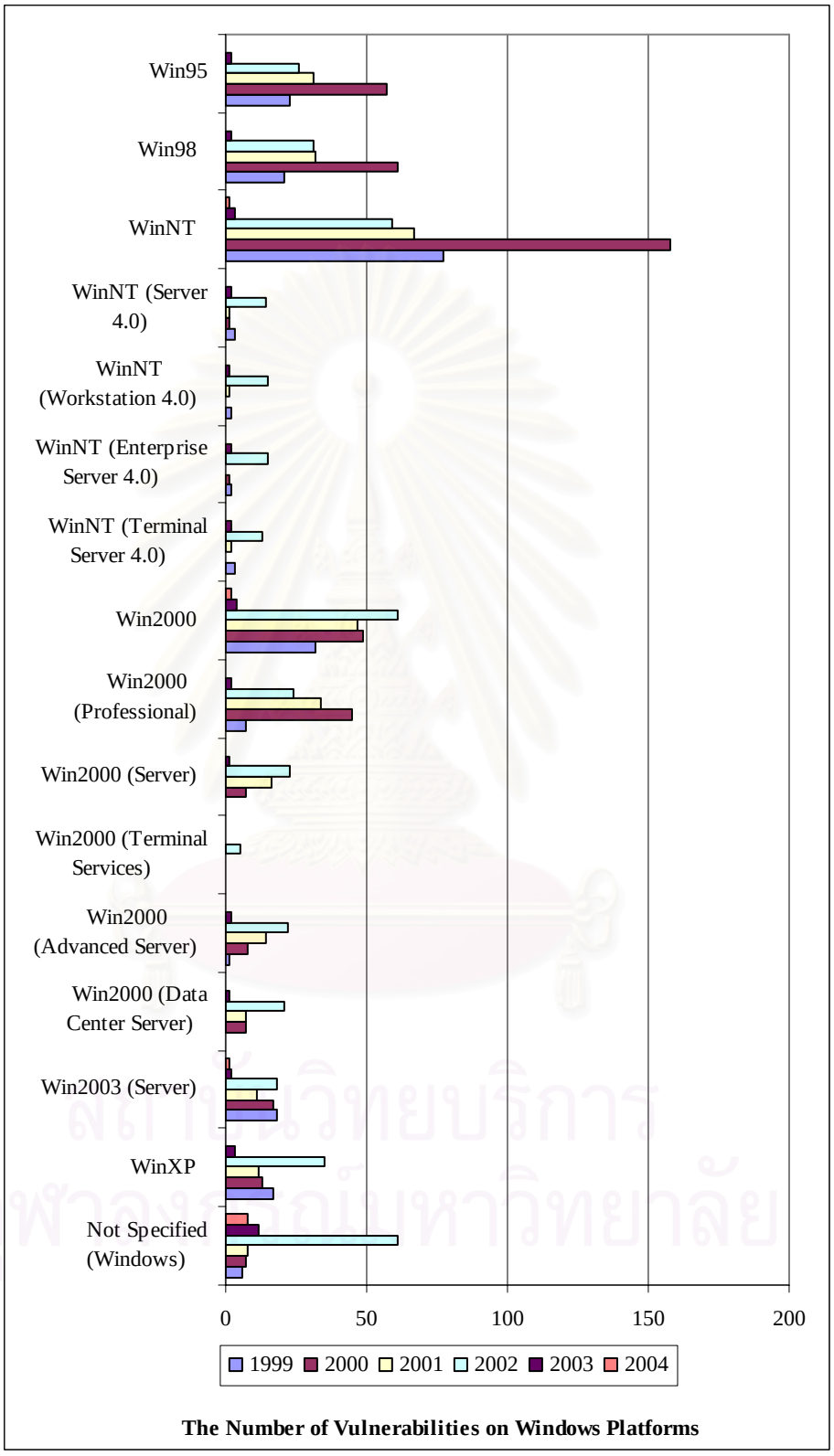
รูปที่ 5.29 – 5.32 จะแสดงรายการจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์ของระบบปฏิบัติการเช่นเดียวกันกับรูปที่ 5.25 – 5.28 แต่จะแสดงรายละเอียดการเกิดจุดอ่อนที่เกิดขึ้นในแต่ละปี ตั้งแต่ปี 1999 – 2004



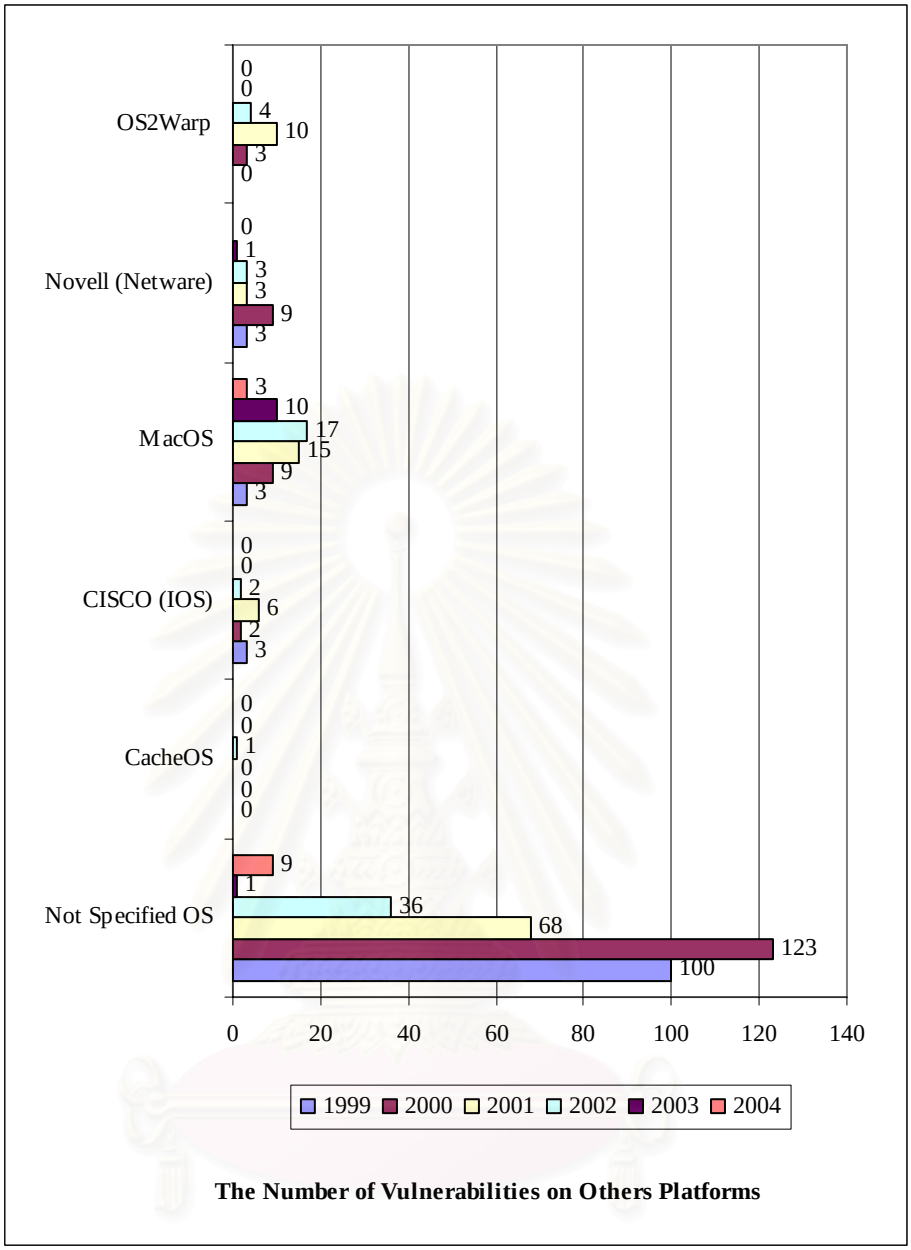
รูปที่ 5.29 **กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์แยกตามประเภทของระบบปฏิบัติการยูนิกซ์และปีที่เกิดจุดอ่อน**



รูปที่ 5.30 กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์แยกตามประเภทของระบบปฏิบัติการลินุกซ์และปีที่เกิดจุดอ่อน



รูปที่ 5.31 กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์แยกตามประเภทของระบบปฏิบัติการวินโดวส์และปีที่เกิดจุดอ่อน



รูปที่ 5.32 กราฟแสดงจำนวนจุดอ่อนบนเซิร์ฟเวอร์แยกตามประเภทของระบบปฏิบัติการอื่น ๆและปีที่เกิดจุดอ่อน

5.2.4 ประเมินและเปรียบเทียบความเปราะบางต่อการโจมตีบนเซิร์ฟเวอร์ของระบบปฏิบัติการประเภทต่าง ๆ

เมื่อทราบแล้วว่าจุดอ่อนที่เกิดขึ้นบนเซิร์ฟเวอร์นั้นมักจะมีลักษณะและตำแหน่งที่เกิดจุดอ่อนเป็นอย่างไร รวมถึงลักษณะความเสียหายและความเปราะบางต่างๆที่มีอยู่ ในส่วนนี้จะแสดงให้เห็นถึงความเปราะบางของเซิร์ฟเวอร์ที่ทำงานบนระบบปฏิบัติการต่างๆ ว่าถ้าหากต้องการเลือกใช้เซิร์ฟเวอร์เพื่อให้บริการแก่ผู้ใช้งานแล้วควรจะเลือกใช้เซิร์ฟเวอร์ที่ทำงานบน

ระบบปฏิบัติการใดจึงจะแข็งแรงน่าเชื่อถือ และระบบปฏิบัติการใดจะมีความเปราะบางสามารถถูกโจมตีจากผู้ไม่หวังดีได้มากน้อยกว่ากัน

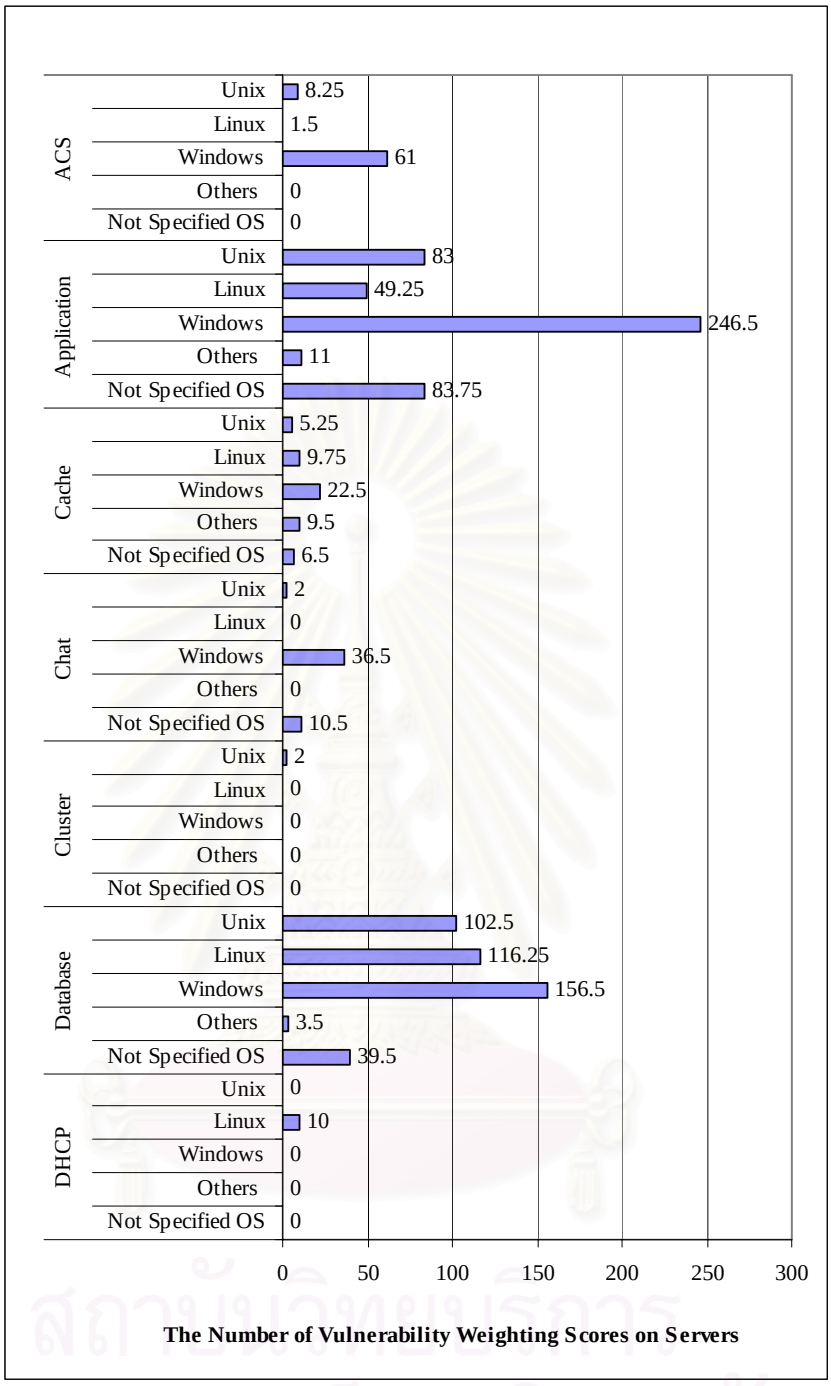
ในการประเมินและเปรียบเทียบความเปราะบางต่อการโจมตีบนเซิร์ฟเวอร์ของระบบปฏิบัติการประเภทต่างๆนี้ จะเปรียบเทียบเพื่อแสดงให้เห็นว่าเซิร์ฟเวอร์ต่างๆเมื่อทำงานบนระบบปฏิบัติการใดจะมีความเปราะบางต่อการถูกโจมตี และมีโอกาสเสี่ยงต่อความเสียหายได้มากน้อยกว่ากัน โดยจะแสดงในรูปแบบของกราฟซึ่งประกอบไปด้วยกราฟต่างๆดังต่อไปนี้

1. กราฟเปรียบเทียบคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการต่างๆ (รูปที่ 5.33 - 5.36)
2. กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการประเภทต่างๆ (รูปที่ 5.37)
3. กราฟแสดงอัตราส่วนร้อยละของความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการประเภทต่างๆ (รูปที่ 5.38)
4. กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการยูนิกซ์ (รูปที่ 5.39)
5. กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการลินุกซ์ (รูปที่ 5.40)
6. กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการวินโดวส์ (รูปที่ 5.41)
7. กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการอื่นๆและที่ไม่มีการระบุไว้ในรายการอ้างอิง (รูปที่ 5.42)
8. กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการยูนิกซ์แยกตามปีที่เกิดจุดอ่อน (รูปที่ 5.43)
9. กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการลินุกซ์แยกตามปีที่เกิดจุดอ่อน (รูปที่ 5.44)

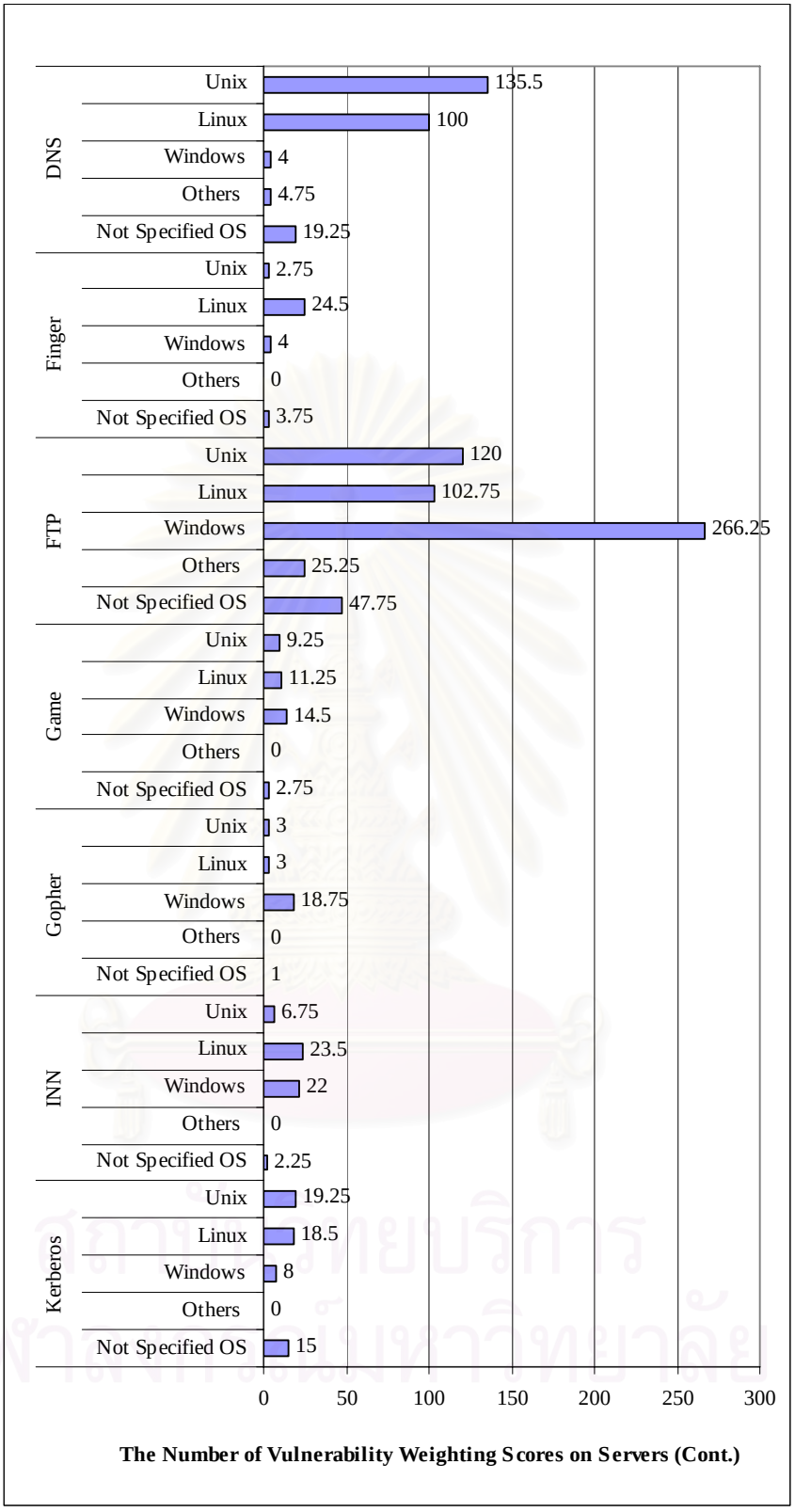
10. กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการวินโดวส์แยกตามปีที่เกิดจุดอ่อน (รูปที่ 5.45)

11. กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการอื่นๆแยกตามปีที่เกิดจุดอ่อน (รูปที่ 5.46)

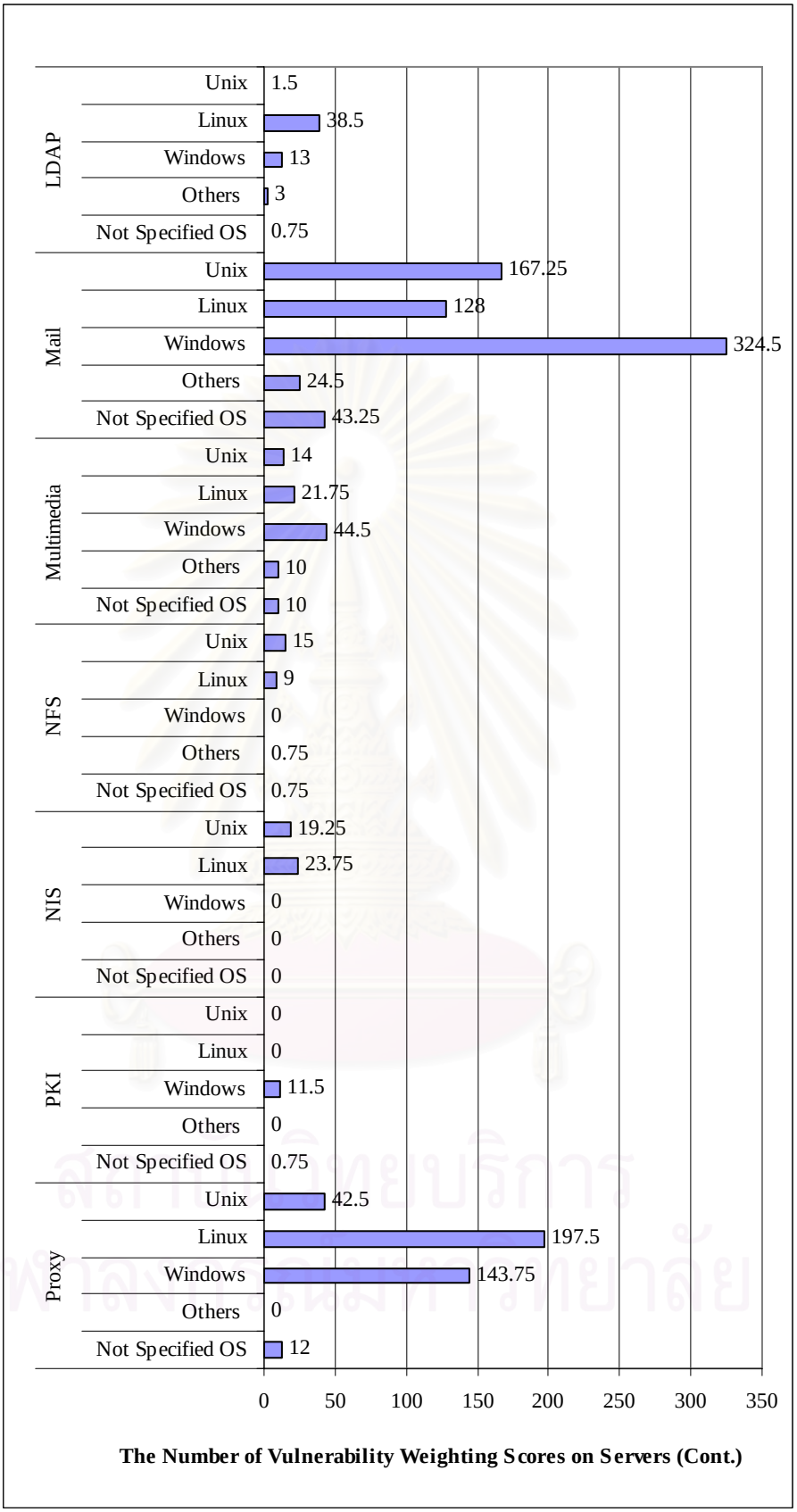
รูปที่ 5.33 – 5.36 แสดงการเปรียบเทียบคะแนนความเปราะบางของแต่ละเซิร์ฟเวอร์แยกตามระบบปฏิบัติการต่างๆ



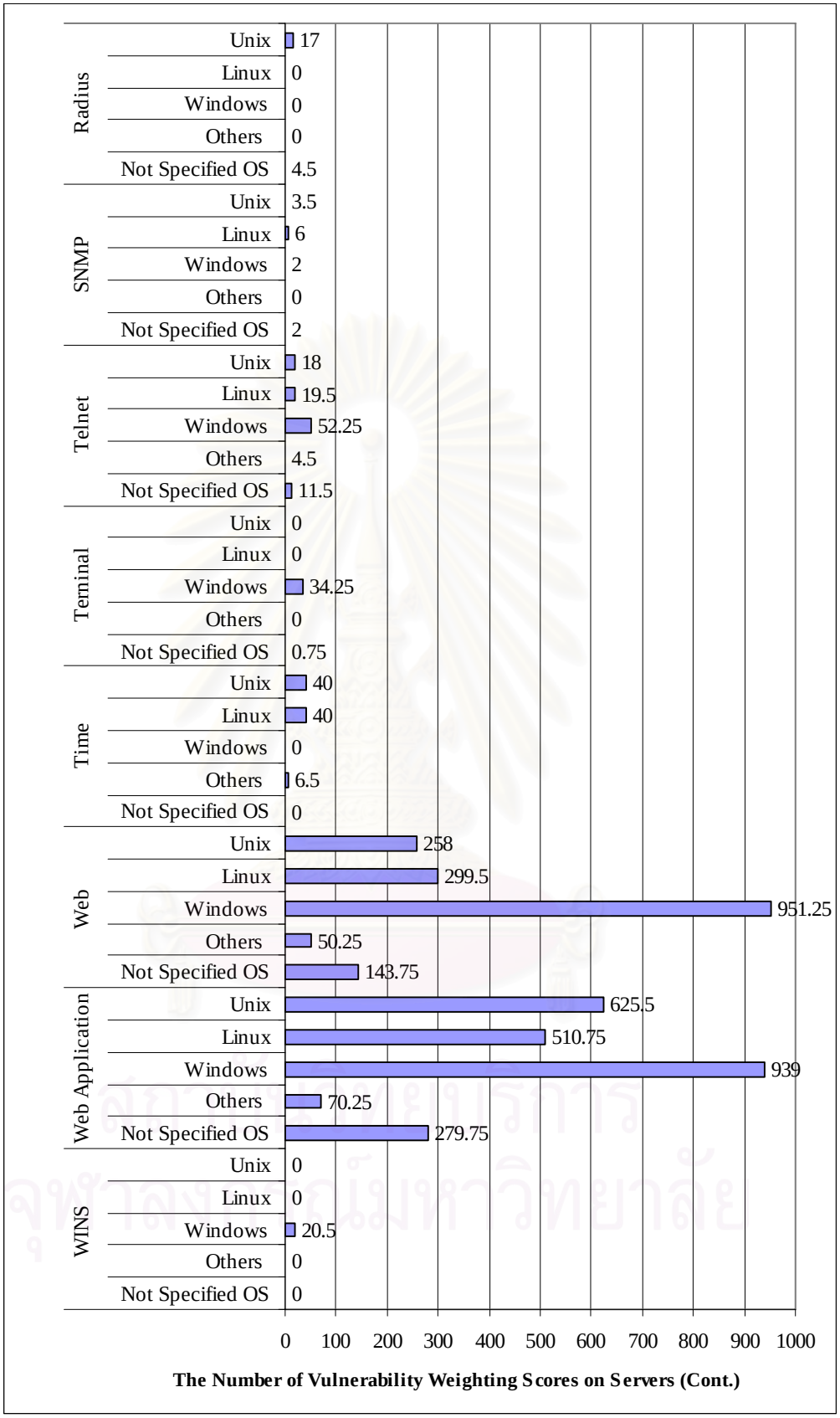
รูปที่ 5.33 **กราฟเปรียบเทียบคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการต่าง ๆ#1**



รูปที่ 5.34 **กราฟเปรียบเทียบคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการต่าง ๆ#2**

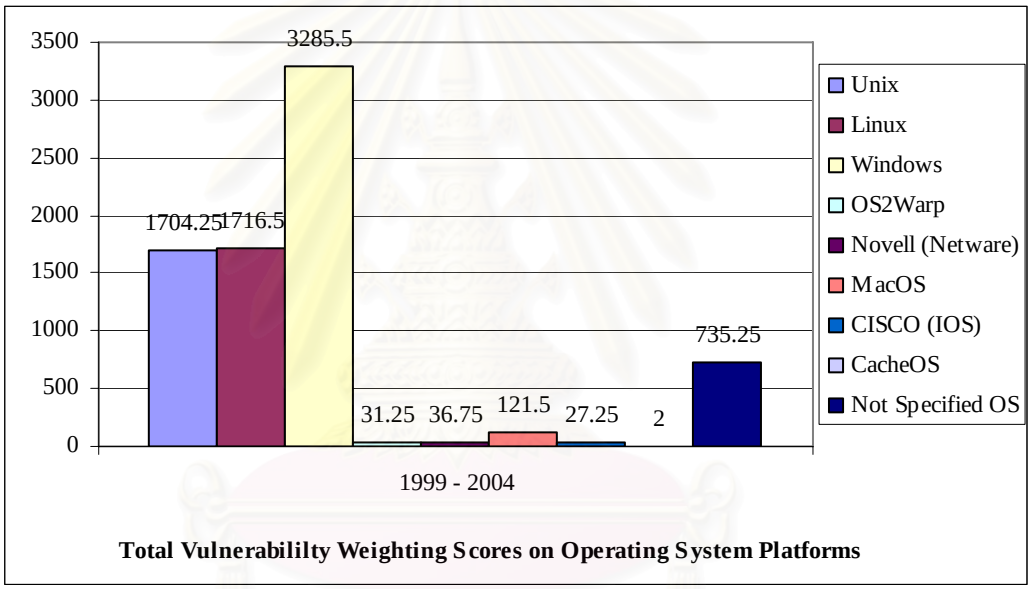


รูปที่ 5.35 กราฟเปรียบเทียบคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการต่าง ๆ#3

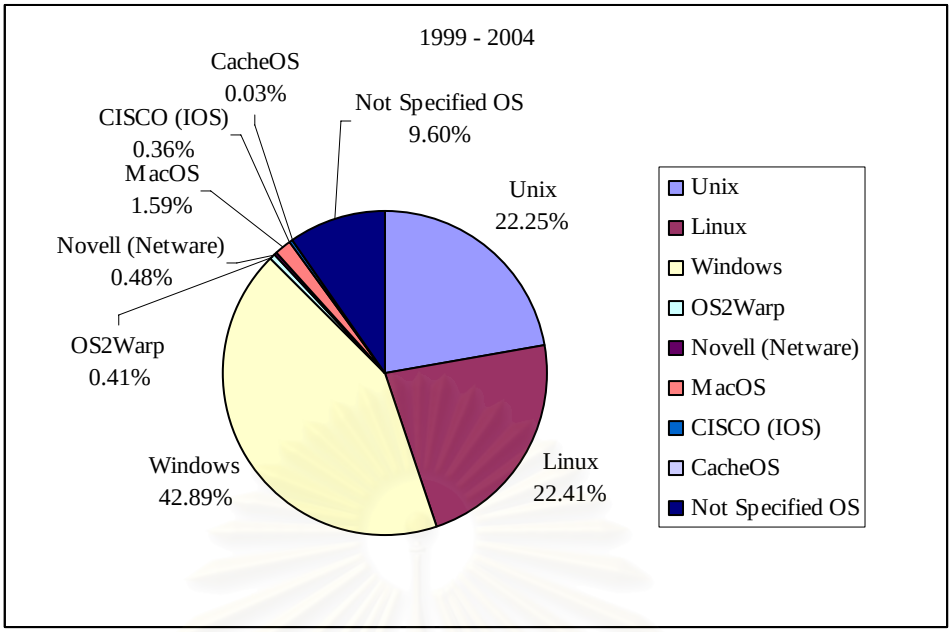


รูปที่ 5.36 **กราฟเปรียบเทียบคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการต่าง ๆ#4**

ในตาราง 5.10 จะแสดงคะแนนความเปราะบางที่เกิดขึ้นของเซิร์ฟเวอร์บนระบบปฏิบัติการต่างๆ โดยแยกตามลักษณะความเสียหายที่เกิดขึ้น เมื่อนำข้อมูลดังกล่าวมาสร้างเป็นกราฟเพื่อให้เห็นผลที่ชัดเจนยิ่งขึ้น จะพบได้ผลว่าเซิร์ฟเวอร์ที่ทำงานบนระบบปฏิบัติการยูนิกซ์ ลินุกซ์ และวินโดวส์ เป็นระบบปฏิบัติการที่มีความเปราะบางสูง โดยเซิร์ฟเวอร์ที่ทำงานบนระบบปฏิบัติการวินโดวส์มีความเปราะบางมากที่สุด โดยคิดเป็นอัตราส่วนร้อยละ 42.89 ในขณะที่เซิร์ฟเวอร์ที่ทำงานบนระบบปฏิบัติการยูนิกส์และลินุกซ์มีความเปราะบางใกล้เคียงกันคือ ร้อยละ 22.25 และ 22.41 ซึ่งระบบปฏิบัติการทั้งสามมีอัตราส่วนความเปราะบางมากถึงร้อยละ 87.55 ของคะแนนความเปราะบางทั้งหมด ดังจะเห็นได้ในรูปที่ 5.37 และ 5.38



รูปที่ 5.37 กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการประเภทต่าง ๆ

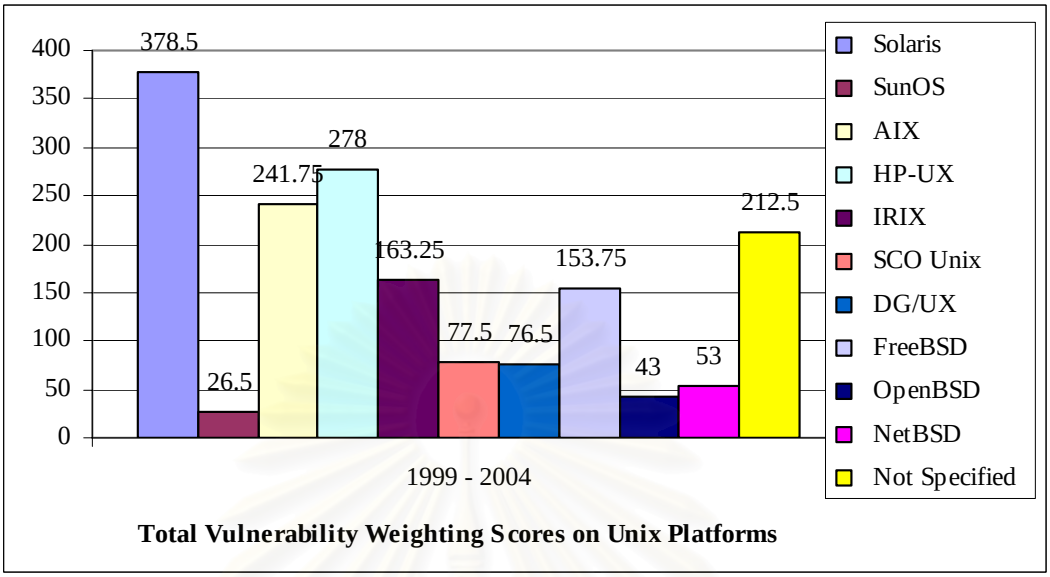


รูปที่ 5.38 กราฟแสดงอัตราส่วนร้อยละของความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการประเภทต่าง ๆ

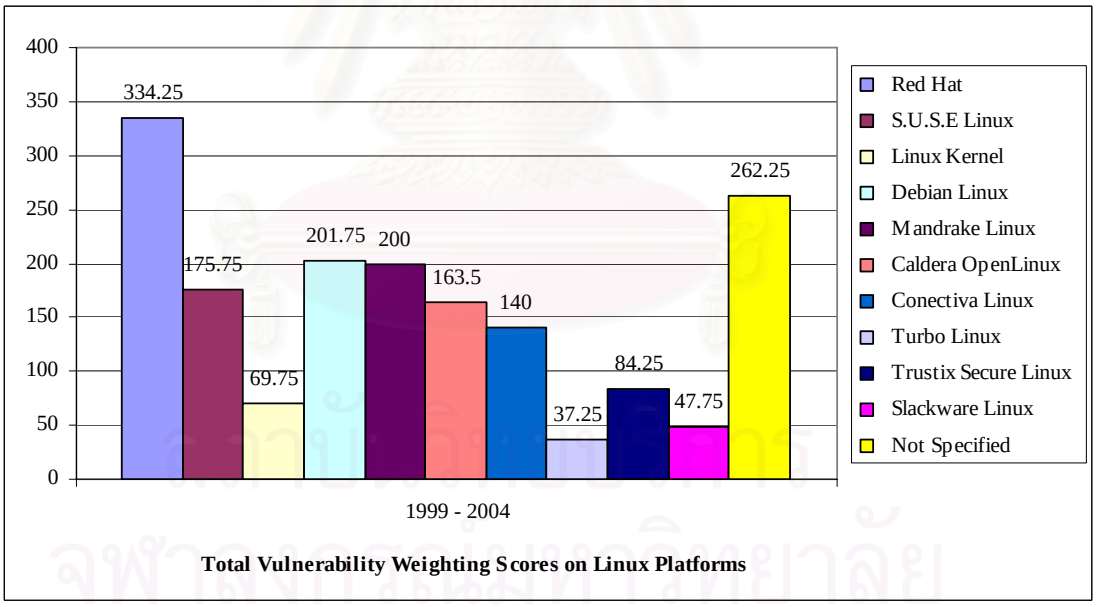
หากเราพิจารณาคะแนนความเปราะบางที่ได้โดยแยกพิจารณาความเปราะบางที่มีของระบบปฏิบัติการประเภทต่างๆ ก็จะได้ผลดังนี้ โดยเซิร์ฟเวอร์ที่ทำงานระบบปฏิบัติการยูนิกซ์ ซันโซลาริส จะมีความเปราะบางต่อการโจมตีมากที่สุด ในขณะที่ถ้าเซิร์ฟเวอร์นั้นใช้ระบบปฏิบัติการลินุกซ์ เรทแฮทลินุกซ์ จะมีความเปราะบางมากที่สุด แต่หาใช้เซิร์ฟเวอร์โดยใช้ระบบปฏิบัติการของค่ายไมโครซอฟต์ วินโดวส์เอ็นทีซึ่งเป็นที่นิยมใช้กันอย่างแพร่หลาย กลับเป็นระบบปฏิบัติการวินโดวส์ที่มีความเปราะบางต่อการโจมตีมากที่สุด ในรูป 5.39 – 5.42 จะแสดงการเปรียบเทียบคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการแต่ละชนิดดังที่กล่าวมาแล้วข้างต้น

Server : All Servers The Number of CVE Entries : 1252						
Platform	Operting System	Loss Type				
		1999 - 2004				
		Confidentiality	Integrity	Availability	System Compromise	Sum
Unix		491	233	601	379.25	1704.25
	Solaris	128	38	137	75.5	378.5
	SunOS	10	2	7	7.5	26.5
	AIX	66	32	91	52.75	241.75
	HP-UX	80	25	115	58	278
	IRIX	50	18	54	41.25	163.25
	SCO Unix	22	5	27	23.5	77.5
	DG/UX	19	6	27	24.5	76.5
	FreeBSD	25	33	58	37.75	153.75
	OpenBSD	13	11	9	10	43
	NetBSD	15	12	17	9	53
	Not Specified	63	51	59	39.5	212.5
Linux		367	378	606	365.5	1716.5
	Red Hat	82	70	111	71.25	334.25
	S.U.S.E Linux	44	42	56	33.75	175.75
	Linux Kernel	19	11	28	11.75	69.75
	Debian Linux	35	43	74	49.75	201.75
	Mandrake Linux	32	48	79	41	200
	Caldera OpenLinux	31	37	58	37.5	163.5
	Conectiva Linux	23	29	64	24	140
	Turbo Linux	4	10	12	11.25	37.25
	Trustix Secure Linux	16	19	36	13.25	84.25
	Slackware Linux	9	7	20	11.75	47.75
	Not Specified	72	62	68	60.25	262.25
Windows		911	644	1263	467.5	3285.5
	Win95	109	40	125	38.5	312.5
	Win98	125	49	128	39.75	341.75
	WinNT	249	129	342	101	821
	WinNT4.0 Server	8	14	20	9.75	51.75
	WinNT4.0 Workstation	5	14	20	9	48
	WinNT4.0 Enterprise Server	8	14	18	9.75	49.75
	WinNT4.0 Terminal Server	5	14	19	9	47
	Win2000	115	62	174	72.25	423.25
	Win2000 Professional	99	61	88	27.5	275.5
	Win2000 Server	20	37	43	15	115
	Win2000 Terminal Services	1	3	8	2.25	14.25
	Win2000 Advanced Server	20	37	39	15.75	111.75
	Win2000 Data Center Server	15	37	29	13	94
	Win2003 Server	44	27	53	32.25	156.25
	WinXP	36	48	75	38.75	197.75
	Not Specified	52	58	82	34	226
OS2	OS2Warp	7	3	13	8.25	31.25
Novell	Netware	4	8	14	10.75	36.75
MacOS	MacOS	29	27	42	23.5	121.5
CISCO	IOS	0	8	11	8.25	27.25
CacheOS	CacheOS	2	0	0	0	2
Not Specified		276	173	184	102.25	735.25
Total Number of Weighting Scores		2087	1474	2734	1365.25	7660.25

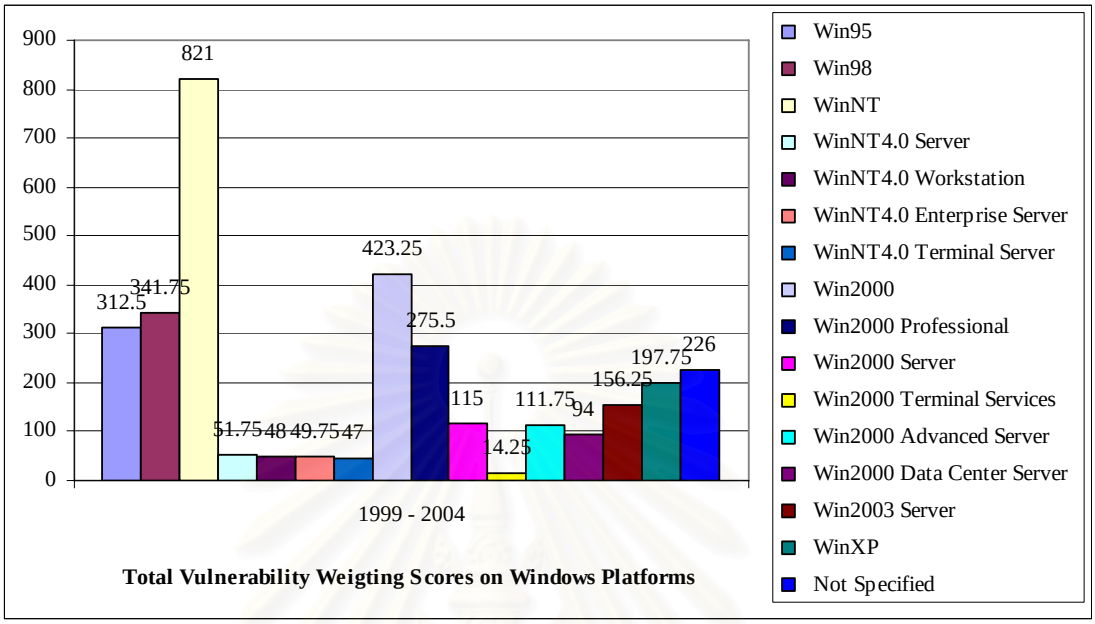
ตารางที่ 5.10 ตารางคะแนนความเปราะบางของเซิร์ฟเวอร์เมื่อเทียบระบบปฏิบัติการและลักษณะความเสียหายที่เกิดขึ้น



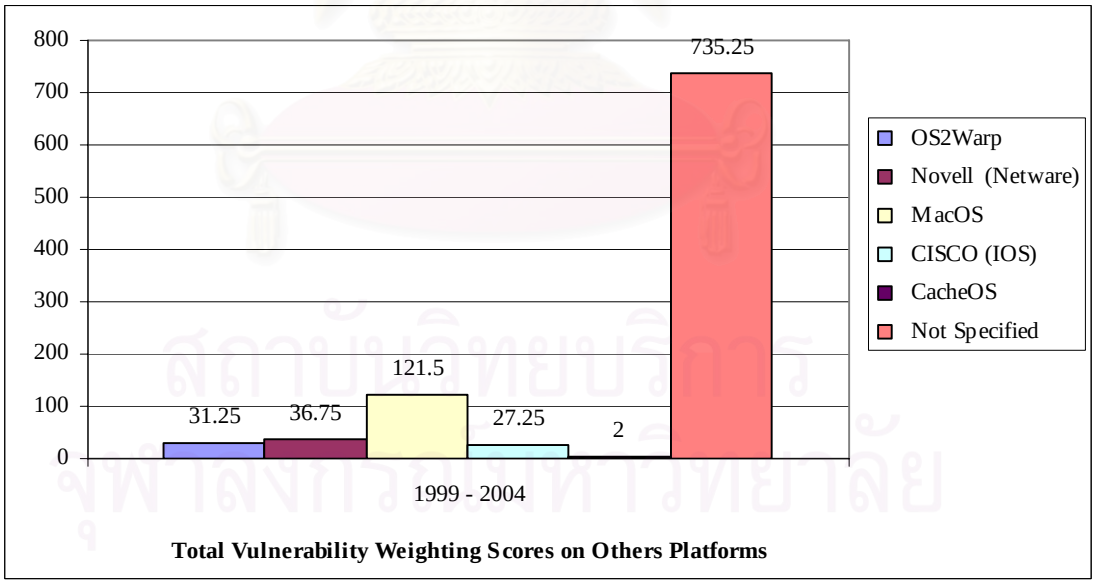
รูปที่ 5.39 กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการยูนิกซ์



รูปที่ 5.40 กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการลินุกซ์

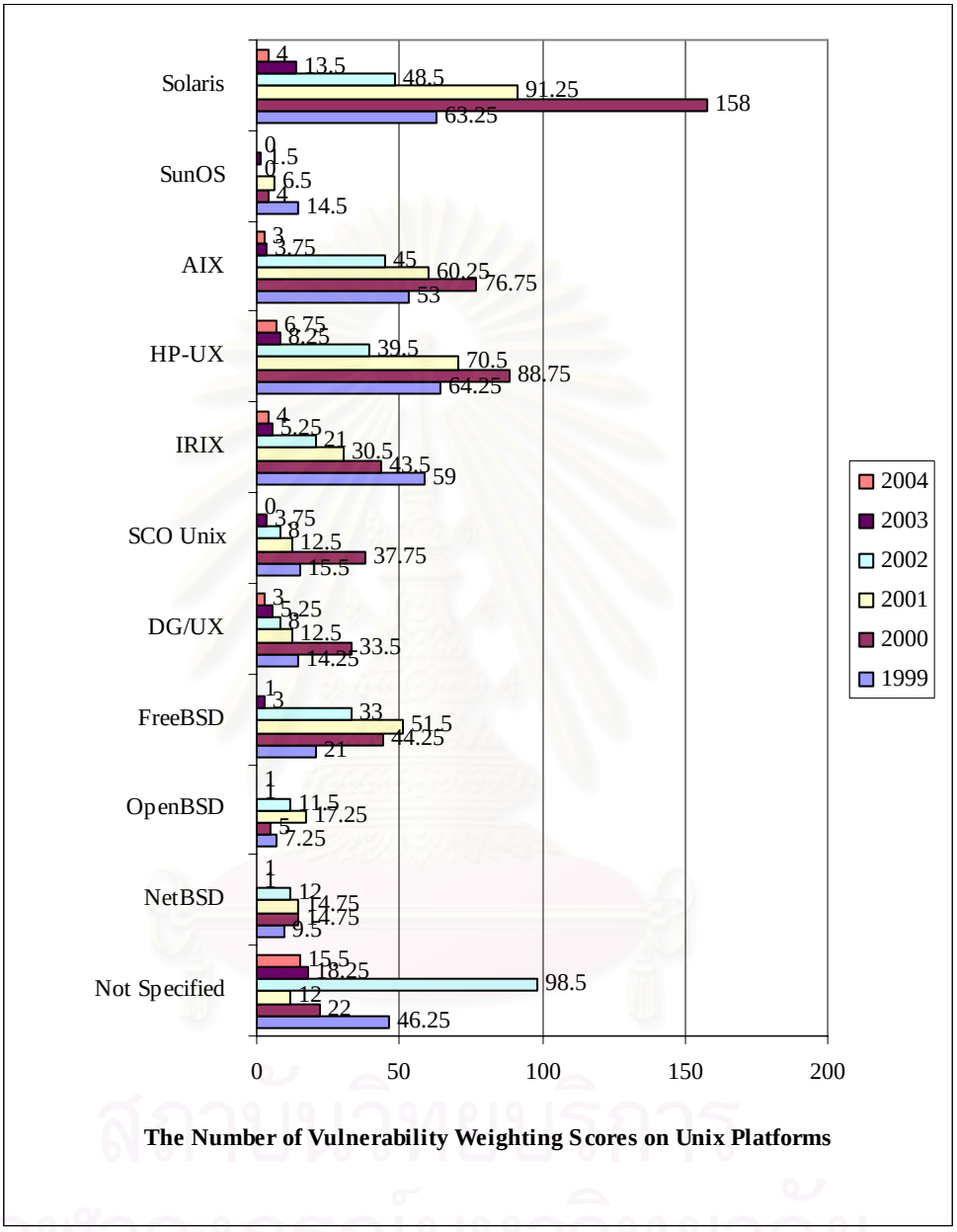


รูปที่ 5.41 **กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการวินโดวส์**

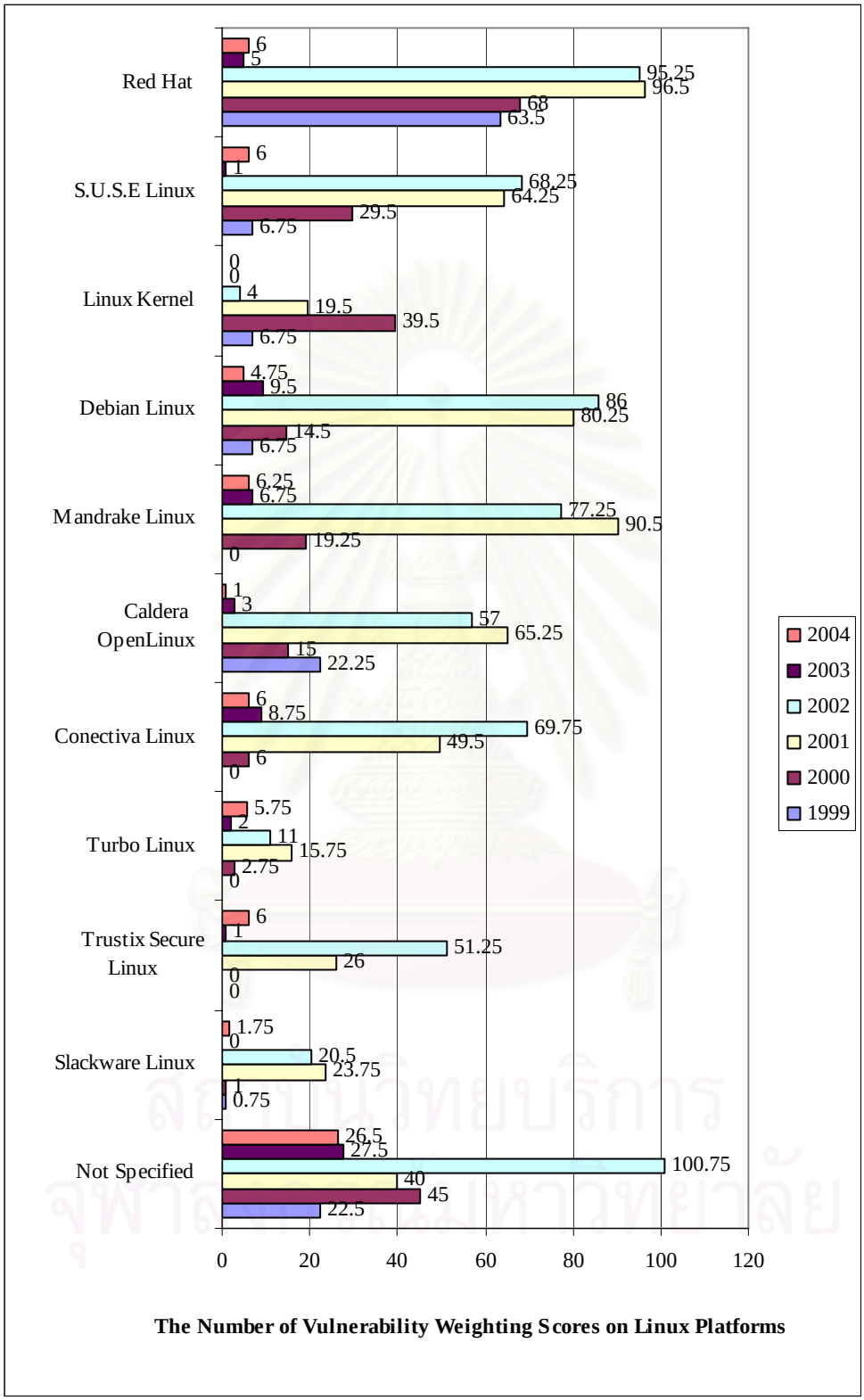


รูปที่ 5.42 **กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการอื่นๆ และที่ไม่มีการระบุไว้ในรายการอ้างอิง**

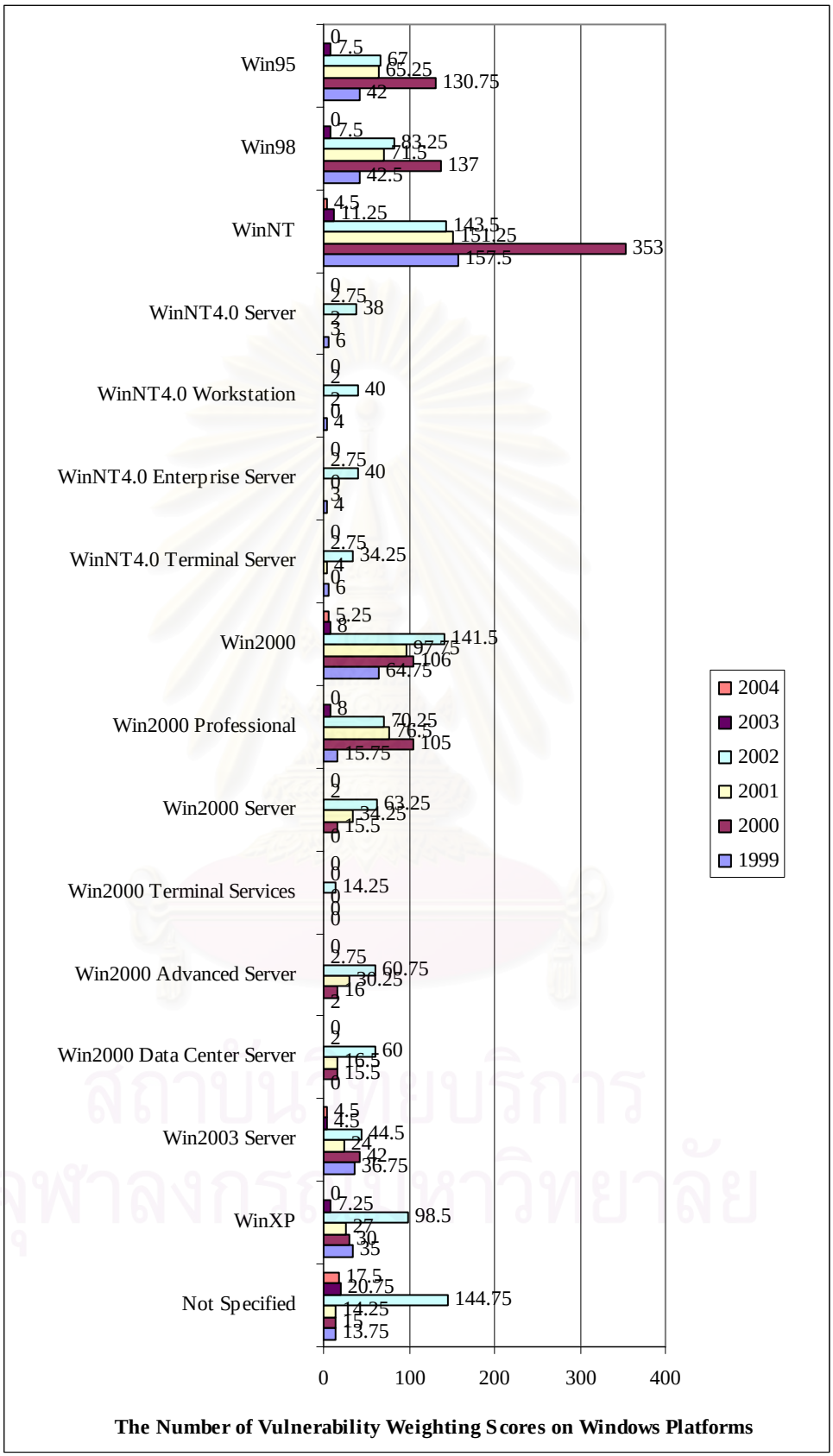
ในรูป 5.43 – 5.46 จะแสดงคะแนนความเปราะบางของระบบปฏิบัติการต่างๆ ในแต่ละปี เพื่อให้สามารถเปรียบเทียบข้อมูลได้อย่างชัดเจนมากยิ่งขึ้น



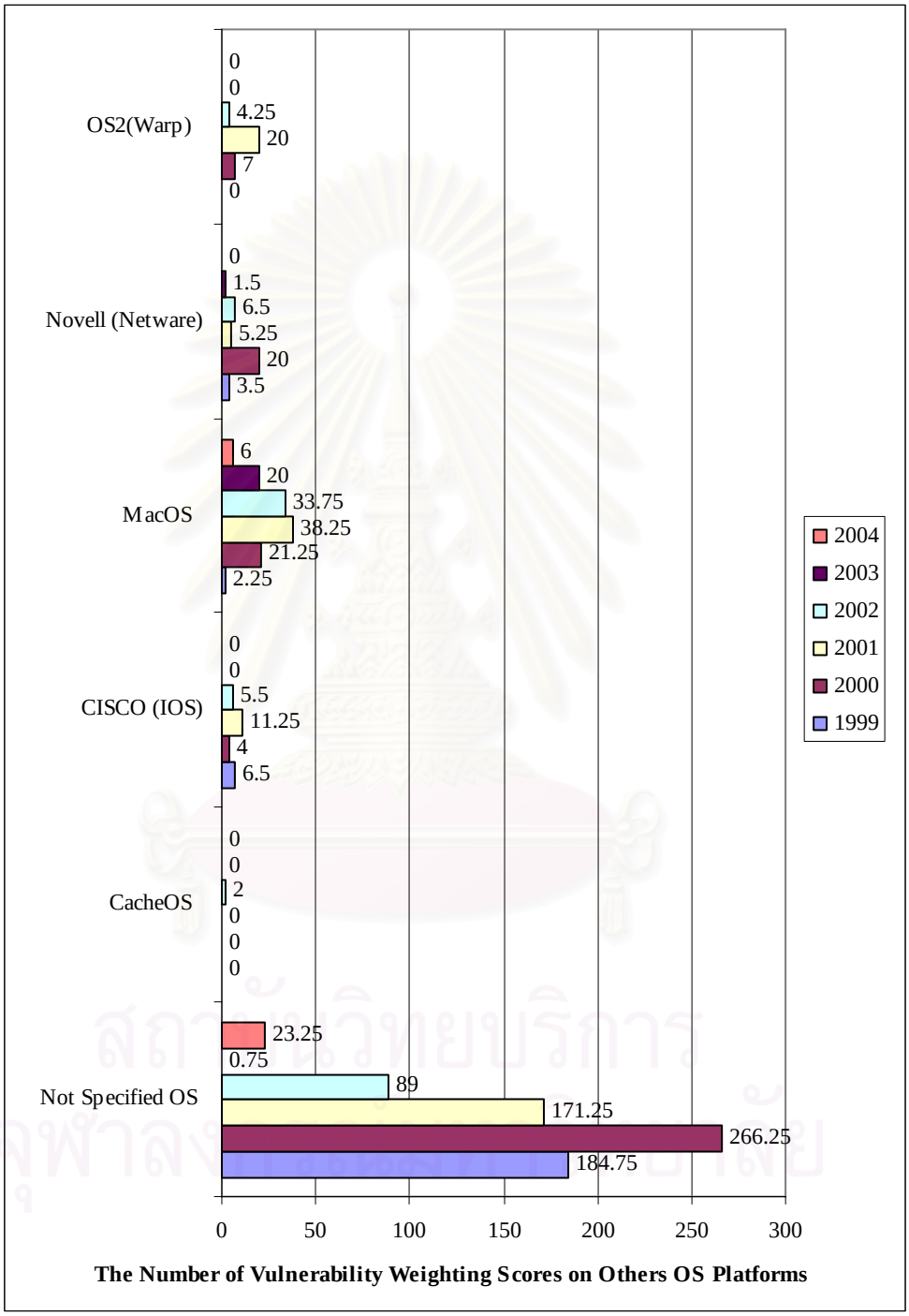
รูปที่ 5.43 กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการยูนิกซ์แยกตามปีที่เกิดจุดอ่อน



รูปที่ 5.44 กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการลินุกซ์แยกตามปีที่เกิดจุดอ่อน



รูปที่ 5.45 กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการวินโดวส์แยกตามปีที่เกิดจุดอ่อน



รูปที่ 5.46 **กราฟแสดงคะแนนความเปราะบางของเซิร์ฟเวอร์บนระบบปฏิบัติการอื่น ๆ แยกตามปีที่เกิดจุดอ่อน**

ในบทที่ 5 ที่ผ่านมา เป็นผลของการดำเนินการวิจัย โดยผลที่ได้ทำให้เห็นแนวโน้มของการเกิดจุดอ่อนและจากการจัดกลุ่มของจุดอ่อนทำให้เห็นลักษณะของจุดอ่อนที่มักจะเกิดขึ้นในระบบคอมพิวเตอร์ ตำแหน่งที่มักจะเกิดจุดอ่อน ลักษณะความเสียหายที่เกิดขึ้น และระบบปฏิบัติการที่ได้รับผลกระทบจากจุดอ่อน อีกทั้งผลคะแนนความเปราะบางที่ได้ทำให้ทราบถึงความเปราะบางต่อการโจมตีบนเซิร์ฟเวอร์และบนระบบปฏิบัติการประเภทต่างๆ ในบทที่ 6 จะทำการสรุปผลการการวิจัยที่ได้ พร้อมทั้งเสนอข้อเสนอแนะบางประการที่มีความสัมพันธ์เกี่ยวข้องกับงานวิจัยนี้ต่อไป

บทที่ 6

สรุปผลการวิจัยและข้อเสนอแนะ

จากการวิเคราะห์จุดอ่อนที่เกิดขึ้นและความเปราะบางจากข้อมูลจุดอ่อนที่มีอยู่บนเซิร์ฟเวอร์ประเภทต่างๆโดยแยกการวิเคราะห์ออกตามระบบปฏิบัติการ ทำให้สามารถสรุปผลการวิจัยได้ดังต่อไปนี้

6.1 สรุปผลการวิจัย

1. เซิร์ฟเวอร์กลุ่มที่พบว่ามีจุดอ่อนมากที่สุดได้แก่ เว็บแอพพลิเคชันเซิร์ฟเวอร์, เว็บเซิร์ฟเวอร์, เมล์เซิร์ฟเวอร์, แอพพลิเคชันเซิร์ฟเวอร์, เอฟทีพีเซิร์ฟเวอร์, ดาต้าเบสเซิร์ฟเวอร์ และพรอกซี่เซิร์ฟเวอร์ เนื่องจากเซิร์ฟเวอร์กลุ่มนี้เป็นกลุ่มที่รองรับการให้บริการแก่ผู้ใช้เป็นจำนวนมาก สามารถเข้าถึงได้โดยง่ายโดยผ่านช่องทางอินเตอร์เน็ต ที่เปรียบเสมือนกับที่สาธารณะที่เป็นที่รู้จักของบุคคลทั่วไปรวมทั้งผู้ที่ไม่หวังดีต่อระบบ ซึ่งทำให้ผู้ที่ไม่หวังดีต่อระบบสามารถหาช่องทางในการโจมตีเซิร์ฟเวอร์ดังกล่าวได้ง่าย ไม่ว่าผู้ที่ไม่หวังดีต่อระบบนั้นจะอยู่ที่ใดในโลกก็ตาม อีกทั้งการโจมตียังเซิร์ฟเวอร์ในกลุ่มดังกล่าวยังจะส่งผลกระทบต่อการให้บริการและการทำงานของผู้ใช้งานเป็นจำนวนมากได้อีกด้วย

2. ความสัมพันธ์ระหว่างจำนวนจุดอ่อนที่เกิดขึ้นและคะแนนความเปราะบางไม่ได้เป็นความสัมพันธ์แบบแปรผันตรงต่อกัน ซึ่งหมายความว่าเซิร์ฟเวอร์ที่มีปริมาณจุดอ่อนเป็นจำนวนน้อยอาจมีโอกาสเสี่ยงหรือความเปราะบางต่อการโจมตีมากกว่าเซิร์ฟเวอร์ที่มีปริมาณจุดอ่อนเป็นจำนวนมากกว่าได้ เช่น เอฟทีพีเซิร์ฟเวอร์ มีปริมาณจุดอ่อนน้อยกว่าแอพพลิเคชันเซิร์ฟเวอร์ แต่กลับมีความเปราะบางต่อการโจมตีมากกว่า

3. ประเภทของจุดอ่อนที่พบมากที่สุดและเป็นช่องทางที่สำคัญสำหรับผู้ไม่หวังดีต่อระบบในการใช้ในการโจมตีได้แก่ จุดอ่อนที่เกิดจากความผิดพลาดในการตรวจสอบข้อมูลนำเข้า

4. จุดที่มักพบจุดอ่อนเกิดขึ้น ได้แก่ ส่วนโปรแกรมสนับสนุนการทำงานของระบบปฏิบัติการ แต่ก็ยังไม่สามารถชี้ชัดลงไปได้ว่าจุดอ่อนที่มีลักษณะเป็นอย่างไรจึงควรจะถูกจัดให้อยู่ในกลุ่มของส่วนโปรแกรมสนับสนุนการทำงานของระบบปฏิบัติการนี้ เนื่องจากงานวิจัยนี้ได้จัดรวมเอาจุดอ่อนที่ไม่เข้าข่ายว่าเป็นจุดอ่อนที่เกิดขึ้นยังจุดที่เกิดจุดอ่อนอื่นใด ได้แก่ ส่วนการเริ่มต้นระบบ, ส่วนการจัดการหน่วยความจำ, ส่วนการจัดการการประมวลผล, ส่วนการจัดการอุปกรณ์, ส่วนการจัดการแฟ้มข้อมูล, ส่วนการพิสูจน์ตัวจริง นำมาจัดรวมอยู่ในส่วนโปรแกรมสนับสนุนการทำงานของระบบปฏิบัติการนี้ โดยถือว่าจุดอ่อนที่ถูกจัดอยู่ในส่วนนี้จะมีความแตกต่างกับจุดอ่อนที่

เกิดขึ้นที่ส่วนโปรแกรมประยุกต์ คือ จุดอ่อนที่ถูกจัดอยู่ในส่วนโปรแกรมสนับสนุนการทำงานของระบบปฏิบัติการนี้มักจะเป็นจุดอ่อนที่เกิดขึ้นกับโปรแกรมหรือซอฟต์แวร์จำพวกที่มีองค์ประกอบที่มีเอกสิทธิ์สูง และมักได้รับสิทธิ์พิเศษบางประการจากระบบปฏิบัติการ ทำให้สันนิษฐานได้ว่าผู้ไม่หวังดีต่อระบบมักจะโจมตีมายังจุดดังกล่าวเนื่องจากหากผู้โจมตีสามารถเจาะระบบเข้ามาในจุดดังกล่าวได้แล้วนั้น ก็อาจจะทำให้ผู้โจมตีสามารถใช้สิทธิ์พิเศษของโปรแกรมนั้น ในการสร้างความเสียหายหรือล่วงละเมิดระบบในส่วนอื่นๆต่อไปได้ ซึ่งผู้ที่จะนำข้อมูลจุดอ่อนที่เกิดขึ้นในส่วนโปรแกรมสนับสนุนการทำงานของระบบปฏิบัติการนี้ไปใช้ อาจจำเป็นจะต้องค้นหาข้อมูลรายละเอียดเพิ่มเติมมากกว่าข้อมูลจุดอ่อนที่ผ่านการจัดกลุ่มคร่าวๆในงานวิจัยนี้

5. เมื่อเทียบความเปราะบางต่อการโจมตีของเซิร์ฟเวอร์โดยพิจารณาจากระบบปฏิบัติการต่างๆ จะสรุปได้ว่า เซิร์ฟเวอร์ที่ทำงานอยู่บนระบบปฏิบัติการวินโดวส์จะมีปริมาณจุดอ่อนและความเปราะบางสูงที่สุด อันจะมีผลทำให้มีโอกาสในการถูกโจมตีจากผู้ไม่หวังดีต่อระบบมากที่สุดเช่นกัน โดยแพลตฟอร์มที่พบว่ามีจุดอ่อนมากที่สุดได้แก่ วินโดวส์เอ็นที ซึ่งเป็นระบบปฏิบัติการที่มีผู้นิยมใช้งาน และเป็นระบบปฏิบัติการที่ออกแบบมาสำหรับเซิร์ฟเวอร์ที่ให้บริการแก่ผู้ใช้งานเป็นปริมาณมากๆ ทั้งนี้เนื่องจากระบบปฏิบัติการวินโดวส์เป็นระบบ ปฏิบัติการที่ได้รับความนิยมแก่ผู้ใช้เป็นจำนวนมาก ดังนั้นระบบปฏิบัติการวินโดวส์จึงน่าจะเป็นระบบปฏิบัติการที่ผู้ไม่หวังดีต่อระบบมักจะทำการเจาะระบบหรือหาช่องทางในการโจมตี เพราะสามารถหาข้อมูลเพื่อใช้ในการโจมตีได้ง่ายและสามารถสร้างความเสียหายให้แก่ผู้ใช้จำนวนมากได้เช่นกัน แต่เมื่อคำนวณเป็นคะแนนความเปราะบางกลับพบว่าแพลตฟอร์มของระบบปฏิบัติการที่มีคะแนนความเปราะบางมากที่สุดได้แก่ ระบบปฏิบัติการในตระกูลวินโดวส์ 2000

6. สำหรับระบบปฏิบัติการประเภทอื่นๆที่สำคัญ ได้แก่ ระบบปฏิบัติการยูนิกซ์และระบบปฏิบัติการลินุกซ์ จากผลงานวิจัยพบว่า ในระบบปฏิบัติการยูนิกซ์ แพลตฟอร์มที่พบว่ามีจุดอ่อนและความเปราะบางมากที่สุด ได้แก่ ระบบปฏิบัติการยูนิกซ์ในตระกูลโซลาริส และลินุกซ์เรดแฮท คือแพลตฟอร์มที่พบว่ามีจุดอ่อนและความเปราะบางมากที่สุดในระบบปฏิบัติการลินุกซ์

7. ผลที่ได้ในงานวิจัยนี้เป็นผลที่ได้จากจุดอ่อนที่เกิดขึ้นในปี 1999 – 2004 ดังนั้นจำนวนจุดอ่อนที่เกิดขึ้นหรือคะแนนความเปราะบางที่ได้ จึงเป็นคะแนนที่สะสมจากระยะเวลาทั้งสิ้น 6 ปี ซึ่งหากพิจารณาจากผลที่ได้ บางเซิร์ฟเวอร์หรือบางระบบปฏิบัติการที่ได้รับผลกระทบอาจจะมีจำนวนจุดอ่อน หรือคะแนนความเปราะบางที่สูงกว่าเซิร์ฟเวอร์หรือระบบปฏิบัติการอื่น แต่หากมองดูจุดอ่อนที่เกิดในปีหลังๆเช่น 2003 – 2004 จะพบว่าเซิร์ฟเวอร์ที่มีปริมาณจุดอ่อนต่างกันนี้อาจมีปริมาณจุดอ่อนที่เกิดขึ้นใกล้เคียงกันหรืออาจไม่มีเลยก็ได้

6.2 ข้อเสนอแนะ

จากผลการวิจัยรวมทั้งสรุปผลที่ได้ มีข้อแนะนำบางประการดังนี้

1. ผลจากงานวิจัยที่ได้สรุปผลออกมาในรูปแบบของกราฟต่างๆ ในงานวิจัยนี้เป็นเพียงการวิเคราะห์มุมมองเพียงส่วนหนึ่งของข้อมูลที่จัดเก็บไว้เท่านั้น หากต้องการวิเคราะห์ข้อมูลให้มีความแม่นยำมากยิ่งขึ้น อาจจะจำเป็นต้องอาศัยมุมมองการวิเคราะห์ข้อมูลในมุมมองอื่นๆที่แตกต่างจากในงานวิจัยนี้ร่วมด้วยเพื่อให้เห็นลักษณะการเกิดจุดอ่อนที่ชัดเจนมากยิ่งขึ้น

2. การพิจารณาเลือกใช้เซิร์ฟเวอร์ในองค์กร การวิเคราะห์ข้อมูลจากจำนวนจุดอ่อนหรือคะแนนความเปราะบางที่ได้เพียงอย่างเดียวอาจจะไม่เพียงพอ เพราะผลลัพธ์ที่ได้อาจจะไม่ใช่ทางเลือกหรือคำตอบที่ดีที่สุดก็เป็นได้หากผู้ที่ทำการวิเคราะห์นั้นขาดความรู้หรือประสบการณ์ที่มากพอ ดังนั้นหากมีผู้ที่มีความรู้ความสามารถหรือผู้ที่มีประสบการณ์ความชำนาญ ช่วยในการวิเคราะห์ข้อมูลก็จะยิ่งช่วยให้สามารถวิเคราะห์ข้อมูลที่เป็นทางเลือกที่ดีที่สุดได้มากยิ่งขึ้น

3. ติดตามผลของจุดอ่อนตามรายการซีวีอีที่เกิดขึ้นในปี ค.ศ. 2005

4. ลดการคำนวณความเปราะบางลงให้เหลือแต่เพียงปีท้ายๆเพื่อเปรียบเทียบและเป็นการให้โอกาสกับแพลตฟอร์มที่มีการปรับปรุงแก้ไขตัวเอง หรืออาจจะมีการให้ค่าถ่วงน้ำหนักที่มากขึ้นสำหรับจุดอ่อนที่เกิดขึ้นในปีท้ายๆ

5. มีรายการจุดอ่อนอยู่เป็นจำนวนมากเช่นกันที่ไม่สามารถระบุได้ว่า จุดอ่อนรายการนั้นๆส่งผลกระทบต่อระบบปฏิบัติการบนแพลตฟอร์มอะไร หรือส่งผลกระทบต่อระบบปฏิบัติการใดบ้าง ซึ่งหากสามารถศึกษาหรือค้นคว้าเพิ่มเติมจนทำให้สามารถระบุถึงประเภทของระบบปฏิบัติการหรือแพลตฟอร์มที่ได้รับผลกระทบจากรายการจุดอ่อนที่เกิดขึ้นในกลุ่มนี้ได้ ก็จะช่วยทำให้จุดอ่อนที่จัดอยู่ในกลุ่มนี้มีจำนวนลดลง และทำให้ได้ข้อมูลระบบปฏิบัติการที่ได้รับผลกระทบจากจุดอ่อนนั้นๆมากขึ้น สามารถนำผลที่ได้ไปวิเคราะห์และประเมินผลได้อย่างถูกต้องมากยิ่งขึ้น

6. แนวโน้มของการเกิดจุดอ่อนในรายการซีวีอีมีแนวโน้มที่ลดลง โดยเฉพาะในปี 2003 – 2004 มีจำนวนลดลงเป็นอย่างมาก แต่ถ้าดูจำนวนจุดอ่อนที่เกิดขึ้นในรายการแคนดิเดดของซีวีอีเวอร์ชั่นล่าสุดคือ 20040901 ซึ่งมีรายการจุดอ่อนอยู่ทั้งหมด 12,505 รายการ พบว่ารายการจุดอ่อนที่ปรากฏในรายการแคนดิเดดกลับไม่ได้มีจำนวนลดลงตามจำนวนรายการจุดอ่อนที่ปรากฏอยู่ในรายการซีวีอี ดังนั้นจึงยังไม่อาจะปักใจเชื่อได้ว่าจำนวนจุดอ่อนที่เกิดขึ้นในระบบคอมพิวเตอร์มีจำนวนลดลง ซึ่งอาจจะต้องมีการศึกษาหาสาเหตุเพิ่มเติมต่อไปว่าทำไมจำนวนจุดอ่อนที่ปรากฏในรายการซีวีอีของปีหลังๆ เช่น ปี 2003 และปี 2004 ถึงได้มีจำนวนลดลงอย่างมาก และในการวิเคราะห์จุดอ่อนที่เกิดขึ้นในระบบคอมพิวเตอร์โดยใช้ข้อมูลจุดอ่อนที่ปรากฏอยู่ในรายการซีวีอีเพียงอย่างเดียวอาจจะทำให้เห็นภาพที่ไม่ชัดเจนต่อการวิเคราะห์ข้อมูล จึงอาจจำเป็น

ที่จะต้องมีการวิเคราะห์ข้อมูลโดยใช้ข้อมูลจุดอ่อนที่ปรากฏในรายการแคดิเดดร่วมด้วย ซึ่งก็จะทำให้สามารถเห็นแนวโน้มของการเกิดจุดอ่อนในภาพรวมได้อย่างชัดเจนมากยิ่งขึ้น

6.3 งานวิจัยในอนาคต

1. การเปรียบเทียบจุดอ่อนต่อการโจมตีโดยมุ่งเน้นที่ตัวระบบปฏิบัติการต่างๆ

2. การเปรียบเทียบและประเมินจุดอ่อนที่เกิดขึ้นกับโปรแกรมสำหรับเครื่องลูกข่าย (Client Software)และเครื่องแม่ข่าย(Server Software)

3. การเปรียบเทียบจุดอ่อนและการประเมินความสามารถในการป้องกันจุดอ่อนของระบบปฏิบัติการวินโดวส์ในเชิงลึก

รายการอ้างอิง

1. Landwehr, C.E., et al. A Taxonomy of Computer Program Security Flaws. ACM Computing Surveys (CSUR) 26(1994): 211 - 254.
2. Jiwnani, K. and Zelkowitz, M. Maintaining Software with a Security Perspective. Proceedings of IEEE International Conference on Software Maintenance (ICSM'02). 2002.
3. รัศมีทิพย์ วิตา. การประเมินและเปรียบเทียบการป้องกันจุดอ่อนของระบบลินุกซ์โดยการเพิ่มความแข็งแกร่งกับการใช้แอลเอสเอ็ม. วิทยานิพนธ์ปริญญามหาบัณฑิต, ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2546.
4. Get CVE. [Online]. Available from: http://www.cve.mitre.org/cve[2004, December 20]
5. CVE Reference Key. [Online]. Available from: http://www.cve.mitre.org/cve/refs/refkey.html[2004, December 23]
6. ICAT Metabase A CVE Based Vulnerability Database. [Online]. Available from: http://icat.nist.gov/icat.cfm[2004, December 23]
7. Internet Security Systems. [Online]. Available from: http://xforce.iss.net[2004, December 23]
8. Securityfocus. [Online]. Available from: http://www.securityfocus.com[2004, December 23]
9. OSVDB The Open Source Vulnerability Database. [Online]. Available from: http://www.osvdb.org[2005, February 10]
10. Common Vulnerabilities and Exposures. [Online]. Available from: http://cve.mitre.org[2004, December 15]
11. เกียรติ ภิรมย์โสภา. การประเมินความเสี่ยงเว็บเซิร์ฟเวอร์โดยการจำแนกระดับผลกระทบของความเสียหาย. วิทยานิพนธ์ปริญญามหาบัณฑิต, ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2547.
12. Alves-Foss, J. and Barbosa, S. Assessing computer security vulnerability. ACM SIGOPS Operating Systems Review 29(1995): 3 – 13.

ประวัติผู้เขียนวิทยานิพนธ์

นาย ไกรสีห์ อัญชนานนท์ เกิดเมื่อวันที่ 15 พฤษภาคม พ.ศ. 2518 เรียนจบการศึกษาระดับมัธยมศึกษาตอนปลายจากโรงเรียน สามเสนวิทยาลัย เข้ารับการศึกษาต่อในระดับปริญญาบัณฑิตที่มหาวิทยาลัยธรรมศาสตร์ ในคณะวิทยาศาสตร์ สาขาวิชาวิทยาการคอมพิวเตอร์ ภาควิชาวิทยาศาสตร์คอมพิวเตอร์ และสำเร็จการศึกษาในระดับปริญญาบัณฑิตในปี พ.ศ. 2541