



ความปลอดภัยคอมพิวเตอร์ (424) การรายงานช่องโหว่ (Vulnerability)

สำหรับนักศึกษาชั้นปีที่ 4 สาขาวิชาวิศวกรรมคอมพิวเตอร์

กรงฤทธิ์ กิติศรีวงศ์พันธุ์
Email : songrit@npu.ac.th
สาขาวิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนครพนม

Revised 2020-06-26

Lecture plan

- 1.1 ข้อมูลเบื้องต้น
- **1.2 ชนิดช่องโหว่ด้านความปลอดภัย**
- 1.3 ชนิดการโจมตี
- 1.4 แรงจูงใจผู้ร้าย
- 1.5 ตัวอย่างการโจมตี: shellshock

Common Vulnerabilities and Exposures

- Common Vulnerabilities and Exposures (CVE)
- ປີ 1999 ມີຍິນດານ [mitre.org](https://cve.mitre.org)
- ຈັດກຳຈໍານຸ້າຂອ້ມູນປະກາດຕົວລະອົບໄວ້ໃຫ້ສາරຸນຊນທາບ
- ມີຮູບແບບ **CVE-ປີ-ເລຂລຳດັບ**
 - CVE-1999-0067
- ປັຈຈຸບັນເປັນມາຕຣຈໍານກລາງໃນການປະກາດຕົວລະອົບໄວ້ຊອົບເວົ້ວ
- <https://cve.mitre.org>



รายละเอียด CVE

- คำอธิบายช่องโหว่
- ระดับความรุนแรง (CVSS)
- แหล่งอ้างอิง
- วันที่รายงาน

รายละเอียด CVE

- Common Vulnerability Scoring System
- CVSS v3.1 ระดับความรุนแรง (Severity) จาก 0 ถึง 10

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N) Adjacent Network (AV:A) Local (AV:L) Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L) High (AC:H)

Privileges Required (PR)*

None (PR:N) Low (PR:L) High (PR:H)

User Interaction (UI)*

None (UI:N) Required (UI:R)

Scope (S)*

Unchanged (S:U) Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N) Low (C:L) High (C:H)

Integrity Impact (I)*

None (I:N) Low (I:L) High (I:H)

Availability Impact (A)*

None (A:N) Low (A:L) High (A:H)

การคำนวณ ระดับความรุนแรง (Severity)

- <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator>

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N) Adjacent Network (AV:A) Local (AV:L) Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L) High (AC:H)

Privileges Required (PR)*

None (PR:N) Low (PR:L) High (PR:H)

User Interaction (UI)*

None (UI:N) Required (UI:R)

Scope (S)*

Unchanged (S:U) Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N) Low (C:L) High (C:H)

Integrity Impact (I)*

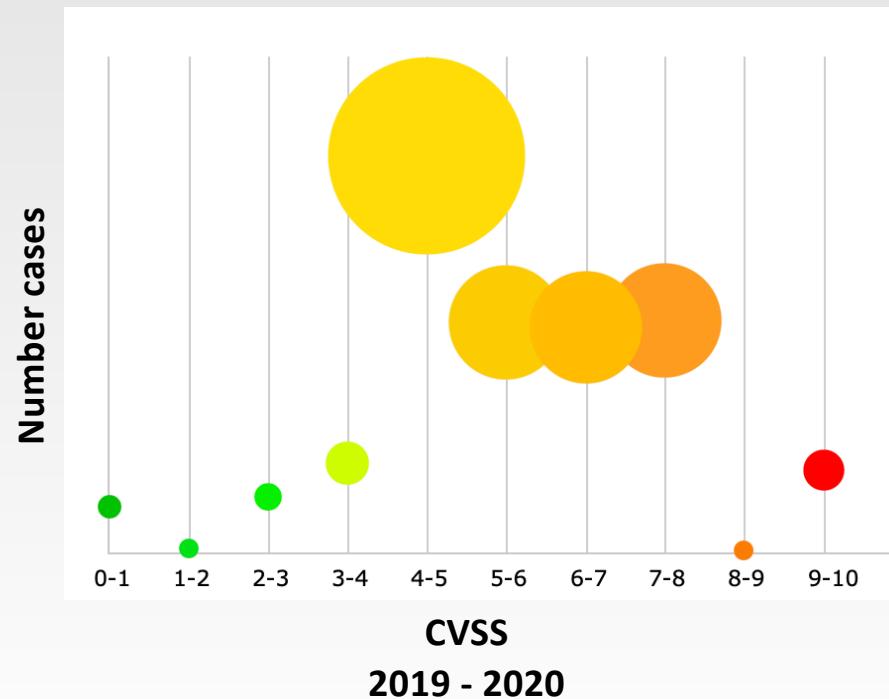
None (I:N) Low (I:L) High (I:H)

Availability Impact (A)*

None (A:N) Low (A:L) High (A:H)

ระดับความสามารถสร้างความเสียหาย

- Common Vulnerability Scoring System (**CVSS**)
- ตั้งแต่ [0, 10] เรียงจากไม่ก่อความเสียหาย ถึงสร้างความเสียหายสูงสุด



1999–2020 Most severity

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication
1	CVE-1999-0002	119		Overflow	1998-10-12	2009-01-26	10.0	Admin	Remote	Low	Not required
				Buffer overflow in NFS mountd gives root access to remote attackers, mostly in Linux systems.							
2	CVE-1999-0003			Exec Code Overflow	1998-04-01	2018-10-30	10.0	Admin	Remote	Low	Not required
				Execute commands as root via buffer overflow in Tooltalk database server (rpc.ttdbserverd).							
3	CVE-1999-0005			Exec Code Overflow	1998-07-20	2008-09-09	10.0	Admin	Remote	Low	Not required
				Arbitrary command execution via IMAP buffer overflow in authenticate command.							
4	CVE-1999-0006			Overflow	1998-07-14	2008-09-09	10.0	Admin	Remote	Low	Not required
				Buffer overflow in POP servers based on BSD/Qualcomm's qpopper allows remote attackers to gain root access using a long PASS command.							
5	CVE-1999-0008			Overflow	1998-06-08	2018-10-30	10.0	Admin	Remote	Low	Not required
				Buffer overflow in NIS+, in Sun's rpc.nisd program.							
6	CVE-1999-0009			Overflow	1998-04-08	2018-10-30	10.0	Admin	Remote	Low	Not required
				Inverse query buffer overflow in BIND 4.9 and BIND 8 Releases.							
7	CVE-1999-0011			DoS	1998-04-08	2018-10-30	10.0	None	Remote	Low	Not required
				Denial of Service vulnerabilities in BIND 4.9 and BIND 8 Releases via CNAME record and zone transfer.							
8	CVE-1999-0018			Overflow	1997-12-05	2018-10-30	10.0	Admin	Remote	Low	Not required
				Buffer overflow in statd allows root privileges.							
9	CVE-1999-0042			Overflow	1997-04-07	2008-09-09	10.0	Admin	Remote	Low	Not required
				Buffer overflow in University of Washington's implementation of IMAP and POP servers.							
10	CVE-1999-0043			Exec Code	1996-12-04	2008-09-09	10.0	Admin	Remote	Low	Not required
				Command execution via shell metachars in INN daemon (innd) 1.5 using "newgroup" and "rmgroup" control messages, and others.							

ชนิดช่องโหว่ด้านความปลอดภัย

- Code Execution
- Memory Corruption
- การใช้หน่วยความจำเกินขนาด (Buffer overflow)
- การยกระดับสิทธิ (Gain Privileges)
- การเชื่อมต่อระยะไกล (Remote Code Execution)
- Denial-of-Service