แจ้งเตือน : ช่องโหว่

ระดับ : High

ผลกระทบทางธุรกิจ
- ☒ Financial Damage
- ☒ Reputation Damage
- ☐ Non-Compliance
- ☐ Privacy Violation

ผลกระทบต่อระบบ
- ☐ Loss of Confidentiality
- ☐ Loss of Integrity
- ☒ Loss of Availability

TLP Color : White

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนช่องโหว่ระดับสูง (High) จากจากการใช้ไลบรารี OpenSSL สำหรับการเข้ารหัสการรับส่งข้อมูลเครือข่ายโดยใช้โปรโตคอล SSL และ TLS (CVE-2022-0778)

วันที่แจ้งเตือน 7 เมษายน 2565

ตามที่ปรากฏเป็นข่าวแจ้งเตือนเกี่ยวกับช่องโหว่ระดับสูง (High) จากการใช้ไลบรารี OpenSSL สำหรับการเข้ารหัสการรับส่งข้อมูลเครือข่ายโดยใช้โปรโตคอล SSL และ TLS (CVE-2022-0778) ทำให้ผู้ไม่หวังดีใช้ช่องโหว่ของฟังก์ชั่น BN_mod_sqrt () ที่ใช้สำหรับประมวลผลการเข้า/ถอดรหัสหรือตรวจสอบใบรับรองที่ใช้ Elliptic Curve Public Key ส่งผลให้เกิดข้อผิดพลาดในการทำงานแบบไม่รู้จบ (Infinite Loop) เป็นเหตุให้ซอฟต์แวร์ อุปกรณ์รักษาความปลอดภัยและอุปกรณ์เครือข่ายที่ใช้ OpenSSL ที่ได้รับผลกระทบสามารถถูกโจมตีแบบ Denial of Service (DOS) ได้

นักวิจัยด้านการรักษาความปลอดภัยได้ทำการ Proof of Concept (POC) แล้วพบว่าช่องโหว่ดังกล่าว **สามารถใช้งานได้จริงโดยมีซอฟต์แวร์ อุปกรณ์รักษาความปลอดภัย และอุปกรณ์เครือข่ายที่ได้รับผลกระทบดังนี้**

ซอฟต์แวร์ อุปกรณ์รักษาความปลอดภัย และอุปกรณ์เครือข่าย	เวอร์ชันที่ได้รับผลกระทบ
1. OpenSSL	ตั้งแต่ 1.0.2 – ก่อน 1.0.2zd , 1.1.0 – ก่อน 1.1.0n, 3.0 – ก่อน 3.02
2. Fortinet	FortiOS, FortiManager, FortiAnalyzer, FortiDeceptor, FortiAuthenticator, FortiMail, FortiRecorder, FortiProxy, FortiSwitch, Fortiweb
3. Checkpoint	Site to Site VPN, Remote Access VPN, Mobile Access / SSL VPN, HTTPS Inspection, Quantum Security Management, Multi-Domain Security Management, Quantum Edge, Quantum Scalable Chassis, Quantum Maestro, Quantum Spark Appliances
4. Paloalto (PAN-OS)	ตั้งแต่ 8.1 – ก่อน 8.1.23 ตั้งแต่ 9.0 – ก่อน 9.0.16-hf ตั้งแต่ 9.1 – ก่อน 9.1.13-hf ตั้งแต่ 10.0 – ก่อน 10.0.10 ตั้งแต่ 10.1 – ก่อน 10.1.5-h1 ตั้งแต่ 10.2 – ก่อน 10.2.1
5. F5	BIG-IP, BIG-IQ Centralized Management, F5OS-A, F5OS-C, Traffix SDC
6. ซอฟต์แวร์หรือระบบปฏิบัติการอื่น ๆ ที่ใช้ OpenSSL เวอร์ชันที่ได้รับผลกระทบ เช่น Red Hat Debian และ Ubantu เป็นต้น	

แจ้งเตือน : ช่องโหว่

ระดับ : High

ผลกระทบทางธุรกิจ
- [x] Financial Damage
- [x] Reputation Damage
- [ ] Non-Compliance
- [ ] Privacy Violation

ผลกระทบต่อระบบ
- [ ] Loss of Confidentiality
- [ ] Loss of Integrity
- [x] Loss of Availability

TLP Color : White

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนช่องโหว่ระดับสูง (High) จากจากการใช้ไลบรารี OpenSSL สำหรับการเข้ารหัสการรับส่งข้อมูลเครือข่ายโดยใช้โปรโตคอล SSL และ TLS (CVE-2022-0778)

วันที่แจ้งเตือน 7 เมษายน 2565

เพื่อหลีกเลี่ยงและป้องกันความเสี่ยงที่อาจเกิดขึ้น ผู้ดูแลระบบควรพิจารณาดำเนินการดังนี้

1. ตรวจสอบและพิจารณาอัปเดต Security Patch ของซอฟต์แวร์ อุปกรณ์รักษาความปลอดภัย และอุปกรณ์เครือข่ายที่ได้รับผลกระทบหรือมีการใช้งาน OpenSSL เวอร์ชันดังกล่าว ให้เป็นเวอร์ชั่นล่าสุด เพื่อแก้ไขช่องโหว่ข้างต้นซึ่งสามารถตรวจสอบรายละเอียดเพิ่มเติมได้ที่

External Link

- https://www.openssl.org/source/
- https://www.fortiguard.com/psirt/FG-IR-22-059
- https://supportcenter.us.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk178411
- https://security.paloaltonetworks.com/CVE-2022-0778
- https://support.f5.com/csp/article/K31323265

2. ผู้ดูแลระบบควรประเมินความเสี่ยงและดำเนินการทดสอบการติดตั้ง Security Patch ก่อนนำไปใช้งานจริง

ข้อมูลอ้างอิง

External Link

1) https://nvd.nist.gov/vuln/detail/CVE-2022-0778
2) https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0778
3) https://www.csirt.gov.it/contenuti/rilevata-vulnerabilita-in-openssl-al02-220316-csirt-ita
4) https://www.openssl.org/news/secadv/20220315.txt
5) https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=a466912611aa6cbdf550cd10601390e587451246
6) https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=3118eb64934499d93db3230748a452351d1d9a65
7) https://www.bleepingcomputer.com/news/security/palo-alto-networks-firewalls-vpns-vulnerable-to-openssl-bug/?fbclid=IwAR2jVFfzf3y4AHWeDIq3pXzhXQY-tp0wueV26XRRiWa4wayH7YEf5RYSqcQ