แจ้งเตือน : ช่องโหว่

HIGH

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

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

TLP Color : White

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนเพื่อ Update Patch ซอฟต์แวร์ Cisco ASA และ Cisco FTD แก้ไขช่องโหว่รุนแรง CVE-2022-20866

วันที่แจ้งเตือน 16 สิงหาคม 2565

ตามที่ปรากฏเป็นข่าว Cisco ได้ออกประกาศชุดอัปเดตซอฟต์แวร์ (Patch) เพื่อแก้ไขช่องโหว่ CVE-2022-20866 (คะแนน CVSS : 7.4) ซึ่งได้รับการอธิบายว่าเป็น "logic error“ ของการบริหารจัดการกุญแจเข้ารหัส RSA ที่ถูกจัดเก็บไว้ในหน่วยความจำบนอุปกรณ์ที่ติดตั้งซอฟต์แวร์ Cisco Adaptive Security Appliance (ASA) และ Cisco Firepower Threat Defense (FTD)

โดยช่องโหว่ CVE-2022-20866 ส่งผลให้ผู้ไม่หวังดีสามารถใช้ประโยชน์จากช่องโหว่ผ่านการโจมตีด้วยวิธี Lenstra side-channel attack ไปยังอุปกรณ์เป้าหมาย เพื่อเข้าถึงกุญแจส่วนตัว (RSA private key) และสามารถใช้กุญแจส่วนตัวดังกล่าวเพื่อเลียนแบบให้เสมือนเป็นอุปกรณ์ หรือ เพื่อถอดรหัสการรับส่งข้อมูลของอุปกรณ์ที่ใช้ซอฟต์แวร์ Cisco ASA หรือซอฟต์แวร์ Cisco FTD ได้

ช่องโหว่ดังกล่าวส่งผลกระทบกับซอฟต์แวร์ Cisco ASA เวอร์ชั่น 9.16.1 ขึ้นไป และซอฟต์แวร์ Cisco FTD เวอร์ชั่น 7.0.0 ขึ้นไป โดยมีผลิตภัณฑ์ที่ได้รับผลกระทบดังปรากฏในอ้างอิง 3

นอกจากนี้ Cisco ได้ออก Patch ปรับปรุงแก้ไขช่องโหว่ CVE-2022-20713 (คะแนน CVSS : 4.3) ในคอมโพเนนต์ Clientless SSL VPN (Web VPN) ของซอฟต์แวร์ Cisco Adaptive Security Appliance (ASA) ซึ่งส่งผลให้ผู้ไม่หวังดีสามารถโจมตีจากระยะไกลโดยไม่ผ่านการตรวจสอบสิทธิ ผ่านการโจมตีบนเบราว์เซอร์ เช่น cross-site scripting โดยอุปกรณ์ที่ได้รับผลกระทบคือ อุปกรณ์ที่ใช้งานซอฟต์แวร์ Cisco ASA Software รุ่นก่อนเวอร์ชั่น 9.17(1) ที่เปิดใช้งาน Clientless SSL VPN

เพื่อหลีกเลี่ยงและป้องกันความเสี่ยงที่อาจเกิดขึ้น ผู้ใช้งานและผู้ดูแลระบบ ควรพิจารณาดำเนินการติดตั้ง Patch ตามที่ Cisco ประกาศ โดยผู้ดูแลระบบควรประเมินความเสี่ยงและดำเนินการทดสอบก่อนนำไปใช้งานจริง (อ้างอิง 3)

ข้อมูลอ้างอิง

1) https://thehackernews.com/2022/08/cisco-patches-high-severity.html
2) https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20866
3) https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz