แจ้งเตือน : ช่องโหว่

High

ผลกระทบทางธุรกิจ

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

ผลกระทบต่อระบบ

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

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนช่องโหว่ระดับสูงของซอฟต์แวร์ Cisco ASA / FTD (CVE-2020-3259)

วันที่แจ้งเตือน 1 มีนาคม 2567

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) สกมช. ได้เผยแพร่รายงานกรณีหน่วยงานด้านความมั่นคงทางไซเบอร์ของสหรัฐ (CISA) แจ้งเตือนพบกลุ่ม Akira Ransomware ใช้ประโยชน์จากช่องโหว่ (CVE-2020-3259) ซึ่งมีผลกระทบระดับสูงในซอฟต์แวร์ Cisco Adaptive Security Appliance (ASA) และ Cisco Firepower Threat Defence (FTD) ในการโจมตีเพื่อเรียกค่าไถ่ (Ransomware)

ช่องโหว่ CVE-2020-3259 เป็นช่องโหว่บน web service interface ของซอฟต์แวร์ ASA และ FTD โดยผู้ไม่หวังดีจะส่งคำสั่ง (crafted GET request) ผ่าน web service interface เพื่อขโมยข้อมูลอ่อนไหว (Sensitive data) เช่น ชื่อผู้ใช้งาน (username) และ รหัสผ่าน (password) จากหน่วยความจำของอุปกรณ์ที่ติดตั้งซอฟต์แวร์ที่มีช่องโหว่ดังกล่าว โดยมีการตั้งค่าใช้งาน AnyConnect หรือ WebVPN configuration

ซอฟต์แวร์ ที่ได้รับผลกระทบ มีดังนี้

ASA เวอร์ชัน	FTD เวอร์ชัน
9.8 – 9.8.4.17	6.2.3 - 6.2.3.15
9.9 – 9.9.2.66	6.3.0 – 6.3.0.5
9.10 – 9.10.1.37	6.4.0 – 6.4.0.8
9.12 – 9.12.3.7	6.5.0 – 6.5.0.4
9.13 – 9.13.1.7	

ทั้งนี้ Cisco ได้ออก Patch เพื่อแก้ไขช่องโหว่แล้วตั้งแต่เดือนพฤษภาคม 2563 และ ThaiCERT แนะนำให้ผู้ใชงานอัปเดตซอฟตแวร เปนเวอรชันล่าสุดทันที

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 29 ก.พ. 2567
2) https://securityaffairs.com/159244/cyber-crime/cisa-cisco-cve-2020-3259-akira-ransomware.html
3) https://nvd.nist.gov/vuln/detail/CVE-2020-3259#range-6839690
4) https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-asaftd-info-disclose-9eJtycMB.html#vp