แจ้งเตือน : ช่องโหว่

ระดับ : Critical

ผลกระทบทางธุรกิจ

- ☐ Financial damage
- ☒ Reputation damage
- ☐ Non-compliance
- ☐ Privacy violation

ผลกระทบต่อระบบ

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

TLP Color : White

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนช่องโหว่ระดับร้ายแรง (Critical) จากระบบงานที่มีการติดตั้งหรือใช้ Apache Web Service เป็นส่วนประกอบ (CVE-2021-44790)

วันที่แจ้งเตือน 10 มกราคม 2565

ตามที่ปรากฏเป็นข่าวแจ้งเตือนช่องโหว่ระดับร้ายแรง (Critical) จากระบบงาน ซอฟต์แวร์ อุปกรณ์รักษาความปลอดภัย และอุปกรณ์ Appliance ที่มีการติดตั้งหรือใช้ Apache Web Service เป็นส่วนประกอบ (CVE-2021-44790) ซึ่งทำให้ผู้ไม่หวังดีสามารถส่งคำสั่งประเภท Http Request ที่มีส่วนประกอบเป็นภาษา Lua Script ที่ถูกจัดทำเป็นพิเศษก่อให้เกิดข้อผิดพลาดประเภท Buffer Overflow และใช้ช่องโหว่ดังกล่าวเพื่อจารกรรมข้อมูล หรือเรียกใช้คำสั่งระยะไกลโดยไม่ได้รับอนุญาต (Remote Code Execution) หรือใช้ช่องโหว่เพื่อโจมตีในลักษณะ Denial of Service (DoS) โดยเวอร์ชันที่ได้รับผลกระทบตั้งแต่ 2.4.51 ลงไป

เพื่อหลีกเลี่ยงและป้องกันความเสี่ยงที่อาจเกิดขึ้น ผู้ดูแลระบบควรพิจารณาดำเนินการดังนี้

1. ตรวจสอบรายละเอียดของช่องโหว่ข้างต้นและพิจารณาดำเนินการอัปเดต Security Patch ให้เป็นเวอร์ชันล่าสุดได้แก่ 2.4.52 ซึ่งสามารถศึกษารายละเอียดเพิ่มเติมได้ที่ https://httpd.apache.org/security/vulnerabilities_24.html

2. กรณีที่ซอฟต์แวร์ อุปกรณ์รักษาความปลอดภัย และอุปกรณ์ Appliance ที่ใช้อยู่ภายในองค์กรได้รับผลกระทบจากช่องโหว่ข้างต้นท่านควรดำเนินการติดตามการอัปเดต Security Patch จากบริษัทเจ้าของผลิตภัณฑ์

3. ผู้ดูแลระบบควรประเมินความเสี่ยงและดำเนินการทดสอบการติดตั้ง Security Patch ก่อนนำไปติดตั้งบนระบบที่ให้บริการจริง

ข้อมูลอ้างอิง

1. https://downloads.apache.org/httpd/Announcement2.4.html
2. https://nvd.nist.gov/vuln/detail/CVE-2021-44790
3. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44790
4. https://www.cisa.gov/uscert/ncas/current-activity/2021/12/22/apache-releases-security-update-http-server
5. https://access.redhat.com/security/cve/cve-2021-44790
6. https://security.netapp.com/advisory/ntap-20211224-0001/
7. https://www.debian.org/security/2022/dsa-5035