แจ้งเตือน : ช่องโหว่

ระดับ : High

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

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

TLP Color : White

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนช่องโหว่ระดับสูง (High) จากการใช้งานเครื่องมือบริหารจัดการระบบผ่านเว็บ (Webmin) (CVE-2022-0824)

วันที่แจ้งเตือน 25 มีนาคม 2565

ตามที่ปรากฏเป็นข่าวแจ้งเตือนเกี่ยวกับช่องโหว่ระดับสูง (High) จากการใช้งานเครื่องมือบริหารจัดการระบบผ่านเว็บ (Webmin) ที่ติดตั้งบนระบบปฏิบัติการ Linux และระบบปฏิบัติการที่คล้าย Unix (UNIX-Like) (CVE-2022-0824) โดยเครื่องมือดังกล่าวมีช่องโหว่ที่เปิดโอกาสให้ผู้ไม่หวังดีที่ได้รับสิทธิเข้าถึงระบบ (Authenticated User) ผ่านเครื่องมือ Webmin สามารถยกระดับสิทธิ (Local Privilege Escalation) เป็นสิทธิสูงสุด (Root) เพื่อให้สามารถส่งและเรียกใช้คำสั่งอันตรายจากระยะไกลโดยไม่ได้รับอนุญาต (Remote Code Execution) และเข้าควบคุมระบบ

นักวิจัยด้านการรักษาความปลอดภัยได้ทำการ Proof of Concept (POC) แล้วพบว่าช่องโหว่ดังกล่าว **สามารถใช้งานได้จริงบนเครื่องมือข้างต้น โดยมีเวอร์ชันที่ได้รับผลกระทบได้แก่เวอร์ชัน 1.984 ลงไป**

เพื่อหลีกเลี่ยงและป้องกันความเสี่ยงที่อาจเกิดขึ้น ผู้ดูแลระบบควรพิจารณาดำเนินการดังนี้

1. ตรวจสอบและพิจารณาติดตั้งเครื่องมือ Webmin ให้เป็นเวอร์ชั่นล่าสุด ได้แก่ 1.990 เพื่อแก้ไขช่องโหว่ของเครื่องมือ ซึ่งสามารถตรวจสอบรายละเอียดเพิ่มเติมได้ที่

- https://www.webmin.com/download.html *External Link*

2. ผู้ดูแลระบบควรประเมินความเสี่ยงและดำเนินการทดสอบการติดตั้ง Patch ก่อนนำไปใช้งานจริง

ข้อมูลอ้างอิง

1) https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0824
2) https://nvd.nist.gov/vuln/detail/CVE-2022-0824
3) https://github.com/faisalfs10x/Webmin-CVE-2022-0824-revshell
4) https://huntr.dev/bounties/d0049a96-de90-4b1a-9111-94de1044f295/ *External Link*