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) ของของระบบปฏิบัติการ Linux (CVE-2022-0847) “Dirty Pipe”

วันที่แจ้งเตือน 11 มีนาคม 2565

ตามที่ปรากฏเป็นข่าวแจ้งเตือนช่องโหว่ระดับสูง (High) ของระบบปฏิบัติการ Linux (CVE-2022-0847) “Dirty Pipe” ที่ทำให้ผู้ไม่หวังดีที่ได้รับสิทธิระดับผู้ใช้งานทั่วไป (Local User) สามารถแก้ไขเนื้อหาของไฟล์ใด ๆ แม้จะไม่มีสิทธิเข้าถึง (Privilege Escalation) หรือ ถูกกำหนดสถานะไฟล์ให้เป็นอ่านอย่างเดียวเท่านั้น (Read Only) โดยการใช้ช่องโหว่ในการแก้ไขข้อมูลโดยตรงใน Cache Memory ตลอดจนยังสามารถอาศัยช่องโหว่ดังกล่าวในการ Update ไฟล์บนหน่วยจัดเก็บข้อมูล (Disk) ได้ในบางกรณี

นักวิจัยด้านการรักษาความปลอดภัยได้ Proof of Concept (POC) พบว่าช่องโหว่ดังกล่าวไม่ซับซ้อน**สามารถใช้งานได้จริงบนระบบปฏิบัติการ Linux โดยระบบปฏิบัติการที่ได้รับผลกระทบ ดังนี้**

ระบบปฏิบัติการ	เวอร์ชันที่ได้รับผลกระทบ
1. Linux Kernel	ตั้งแต่ 5.8 – ก่อน 5.10.102 , 5.15. – ก่อน 5.15.25 , ตั้งแต่ 5.16 – ก่อน 5.16.11
2. RedHat Enterprise Linux	4 , 8 – 8.4
3. SUSE	ตั้งแต่ 5.8 ขึ้นไป
4. Ubantu	ตั้งแต่ 20.04.2 ลงไป

เพื่อหลีกเลี่ยงและป้องกันความเสี่ยงที่อาจเกิดขึ้น ผู้ดูแลระบบควรพิจารณาดำเนินการดังนี้

1. ตรวจสอบรายละเอียดของช่องโหว่ข้างต้นและพิจารณาดำเนินการอัปเดต Security Patch จากเจ้าของผลิตภัณฑ์ซึ่งสามารถศึกษารายละเอียดเพิ่มเติมตามรายละเอียดด้านล่าง

   - https://access.redhat.com/security/cve/cve-2022-0847
   - https://www.suse.com/security/cve/CVE-2022-0847.html
   - https://ubuntu.com/security/CVE-2022-0847

   External Link

2. ผู้ดูแลระบบควรประเมินความเสี่ยงและดำเนินการทดสอบการติดตั้ง Security Patch ก่อนนำไปติดตั้งบนระบบที่ให้บริการจริง

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) ของของระบบปฏิบัติการ Linux (CVE-2022-0847) “Dirty Pipe”

วันที่แจ้งเตือน 11 มีนาคม 2565

ข้อมูลอ้างอิง

1. https://nvd.nist.gov/vuln/detail/CVE-2022-0847#match-7701517
2. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0847
3. https://packetstormsecurity.com/files/166229/Dirty-Pipe-Linux-Privilege-Escalation.html
4. https://www.rapid7.com/blog/post/2022/03/09/cve-2022-0847-arbitrary-file-overwrite-vulnerability-in-linux-kernel/

External Link