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) ของโปรแกรม PolicyKit (PolKit's pkexec) ทำให้ผู้ไม่หวังดีสามารถยกระดับสิทธิ (Privilege Escalation) บนระบบปฏิบัติการ Linux (CVE-2021-4034)

วันที่แจ้งเตือน 28 มกราคม 2565

ตามที่ปรากฏเป็นข่าวแจ้งเตือนช่องโหว่ระดับสูง (High) ของโปรแกรม PolicyKit (PolKit's pkexec) บนระบบปฏิบัติการ Linux (CVE-2021-4034) ที่ทำให้ผู้ไม่หวังดีใช้เทคนิคการเรียกใช้คำสั่งแปลกปลอมโดยไม่ได้รับอนุญาต (Arbitrary Code Execution) ส่งผลให้สามารถการยกระดับสิทธิของระบบปฏิบัติการ (Local Privilege Escalation) เป็นสิทธิสูงสุด (Root) ได้

นักวิจัยด้านการรักษาความปลอดภัยได้ทำการ Proof of Concept (POC) แล้วพบว่าช่องโหว่ดังกล่าวไม่ซับซ้อน **สามารถใช้งานได้จริงบนระบบปฏิบัติการ Linux และระบบปฏิบัติการที่คล้าย Unix (UNIX-Like) โดยระบบปฏิบัติการที่ได้รับผลกระทบดังนี้**

ระบบปฏิบัติการ	เวอร์ชันที่ได้รับผลกระทบ
1. ระบบปฏิบัติการ Linux ทุกเวอร์ชันที่ติดตั้งโปรแกรม PolKit	
2.ระบบปฏิบัติการ CentOS ทุกเวอร์ชันที่ติดตั้งโปรแกรม PolKit	
3. ระบบปฏิบัติการ Debian ทุกเวอร์ชันที่ติดตั้งโปรแกรม PolKit	
4. ระบบปฏิบัติการ Fedora Distributions ทุกเวอร์ชัน	
5. RedHat Enterprise Linux	6 , 7, 7.3 – 7.4 ,7.6 – 7.7 , 8 – 8.2 , 8.4
6. Ubantu	14.04, 16.04, 18.04, 20.04, 21.10

เพื่อหลีกเลี่ยงและป้องกันความเสี่ยงที่อาจเกิดขึ้น ผู้ดูแลระบบควรพิจารณาดำเนินการดังนี้

1. ตรวจสอบรายละเอียดของช่องโหว่ข้างต้นและพิจารณาดำเนินการอัปเดต Security Patch จากเจ้าของผลิตภัณฑ์ซึ่งสามารถศึกษารายละเอียดเพิ่มเติมตามรายละเอียดด้านล่าง
   - https://access.redhat.com/security/cve/CVE-2021-4034
   - https://ubuntu.com/security/notices/USN-5252-2 , https://ubuntu.com/security/notices/USN-5252-1
   - https://security-tracker.debian.org/tracker/CVE-2021-4034
2. กรณีมีข้อจำกัดในการติดตั้ง Security Patch สามารถใช้วิธีการเพื่อที่จะลดความเสี่ยงเบื้องต้น (Workaround) จากช่องโหว่ข้างต้นโดยดำเนินการระงับสิทธิ SUID ของโปรแกรม PolKit ได้จาก **คำสั่ง chmod 0755 /usr/bin/pkexec**

แจ้งเตือนช่องโหว่ระดับสูง (High) ของโปรแกรม PolicyKit (PolKit's pkexec) ทำให้ผู้ไม่หวังดีสามารถยกระดับสิทธิ (Privilege Escalation) บนระบบปฏิบัติการ Linux (CVE-2021-4034)

วันที่แจ้งเตือน 28 มกราคม 2565

3. ผู้ดูแลระบบควรประเมินความเสี่ยงจากวิธีการบรรเทาและลดความเสี่ยงและควรดำเนินการทดสอบการติดตั้ง Patch หรือการใช้โปรแกรม Workaround รวมถึงการตั้งค่าการป้องกันบนอุปกรณ์รักษาความปลอดภัย ก่อนนำไปติดตั้งบนระบบที่ให้บริการจริง

ข้อมูลอ้างอิง

1. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4034
2. https://blog.qualys.com/vulnerabilities-threat-research/2022/01/25/pwnkit-local-privilege-escalation-vulnerability-discovered-in-polkits-pkexec-cve-2021-4034
3. https://www.bleepingcomputer.com/news/security/linux-system-service-bug-gives-root-on-all-major-distros-exploit-released/
4. https://www.securityweek.com/polkit-vulnerability-provides-root-privileges-linux-systems