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) จากการใช้ระบบปฏิบัติการของผลิตภัณฑ์ Apple (CVE-2022-22639)

วันที่แจ้งเตือน 7 เมษายน 2565

ตามที่ปรากฏเป็นข่าวแจ้งเตือนเกี่ยวกับช่องโหว่ระดับสูง (High) ภายในระบบปฏิบัติการของผลิตภัณฑ์ Apple (CVE-2022-22639) ที่ทำให้ผู้ไม่หวังดีใช้ช่องโหว่ของกระบวนการสำหรับอัปเดตระบบปฏิบัติการ (SUHelper) ที่จำเป็นต้องใช้สิทธิสูงในการทำงานและสามารถ Bypass กระบวนการป้องกันการแก้ไขความถูกต้องเชื่อถือได้ภายในระบบปฏิบัติการ (System Integrity Protection) ส่งผลผู้ไม่หวังดีสามารถยกระดับสิทธิของระบบปฏิบัติการเป็นสิทธิสูงสุด (Root Privilege Escalation) ได้

นักวิจัยด้านการรักษาความปลอดภัยได้ทำการ Proof of Concept (POC) แล้วพบว่าช่องโหว่ดังกล่าว **สามารถใช้งานได้จริงบนระบบปฏิบัติการของผลิตภัณฑ์ Apple โดยมีเวอร์ชันที่ได้รับผลกระทบดังนี้**

ระบบปฏิบัติการของผลิตภัณฑ์ Apple	เวอร์ชันที่ได้รับผลกระทบ
1. iOS	ก่อน 15.4
2. iPadOs	ก่อน 15.4
3. macOS Monterey	ก่อน 12.3

เพื่อหลีกเลี่ยงและป้องกันความเสี่ยงที่อาจเกิดขึ้น ผู้ดูแลระบบควรพิจารณาดำเนินการดังนี้

1. กรณีมีการระบบปฏิบัติการของผลิตภัณฑ์ Apple ที่ได้รับผลกระทบตามรายการดังกล่าวภายในองค์กรให้ตรวจสอบและพิจารณาติดตั้งโปรแกรมให้เป็นเวอร์ชั่นล่าสุดเพื่อแก้ไขช่องโหว่ข้างต้น
2. ผู้ดูแลระบบควรประเมินความเสี่ยงและดำเนินการทดสอบการติดตั้งโปรแกรมที่เป็นเป็นเวอร์ชั่นล่าสุดก่อนนำไปใช้งานจริง

ข้อมูลอ้างอิง

1) https://nvd.nist.gov/vuln/detail/CVE-2022-22639
2) https://www.trendmicro.com/en_us/research/22/d/macos-suhelper-root-privilege-escalation-vulnerability-a-deep-di.html
3) https://github.com/jhftss/CVE-2022-22639?fbclid=IwAR0GRH3xxG1e_u1U3l0C27_Z6QeuCoakI2owp0u17eOk732DbeoupiaOxrQ
4) https://securityonline.info/poc-exploit-released-for-macos-suhelper-root-privilege-escalation-cve-2022-22639/?fbclid=IwAR0bKw8H5KMKeAzdoOKq-JzfHsDVNZRz6gVURv5hDauhwdsbzuEXZW1MAt4

External Link