แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ

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

TLP Color : CLEAR



ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

ช่องโหว่ในผลิตภัณฑ์ Google, OpenSSH (Sshole) และ SonicWall เสี่ยงถูกใช้ในการโจมตี

วันที่แจ้งเตือน 10 พฤศจิกายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า ช่องโหว่ในผลิตภัณฑ์ Google, OpenSSH (Sshole) และ SonicWall เสี่ยงถูกนำไปใช้ในการโจมตีระบบสารสนเทศขององค์กร ได้แก่

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Google	• **ช่องโหว่ CVE-2026-58868** ในระบบปฏิบัติการ Android เป็นช่องโหว่ประเภท Out-of-Bounds Write ซึ่งเกิดจากข้อผิดพลาดในการจัดการหน่วยความจำภายในฟังก์ชัน onOutputReceived ของไฟล์ FrameDecoder.cpp โดยมีสาเหตุจาก Heap Buffer Overflow ทำให้โปรแกรมเขียนข้อมูลเกินขอบเขตพื้นที่หน่วยความจำที่จัดเตรียมไว้ ส่งผลให้ผู้ไม่หวังดีสามารถเรียกใช้โค้ดบนโทรศัพท์มือถือจากระยะไกล (RCE) โดยไม่จำเป็นต้องให้ผู้ใช้คลิกลิงก์ เปิดไฟล์ หรือดำเนินการใด ๆ • Google แนะนำให้ผู้ใช้ตรวจสอบการอัปเดตความปลอดภัยของอุปกรณ์ หากวันที่อัปเดตเป็น 2026-11-01 หรือใหม่กว่า จะครอบคลุมการแก้ไขช่องโหว่ CVE-2026-58868	ส่งผลกระทบต่อผลิตภัณฑ์ที่ใช้ Android เวอร์ชัน 17, 16-qpr2, 16, 15 และ 14
OpenSSH	• **ช่องโหว่ CVE-2026-123158** เป็นช่องโหว่ประเภท Authentication Bypass ในบริการ OpenSSH Server (Sshole) บนระบบ Linux เกิดจากความผิดพลาดในการประมวลผลรหัสผ่าน ทำให้ผู้โจมตีอาจใช้ช่องโหว่โดยการส่งรหัสผ่านที่มีความยาวเกิน 256 ไบต์ และทำให้ระบบประมวลผลผิดพลาดและยอมรับการเข้าสู่ระบบโดยไม่จำเป็นต้องทราบรหัสผ่านที่ถูกต้อง • ผู้ดูแลระบบควรตรวจสอบ Linux ที่ใช้งานอยู่ใช้ musl libc และปิด PAM หรือไม่ รวมถึงตรวจสอบบัญชีผู้ใช้ที่อนุญาตผ่าน SSH โดยเฉพาะบัญชีที่มีสิทธิสูง และดำเนินการอัปเดต OpenSSH เป็นเวอร์ชัน 10.6p2 ที่ได้รับการแก้ไขแล้ว	ส่งผลกระทบต่อ OpenSSH เวอร์ชันก่อน 10.6p2 บนระบบปฏิบัติการ Linux ที่ใช้ไลบรารี musl libc และปิดการใช้งาน Pluggable Authentication Module (PAM)

ข้อมูลอ้างอิง Google

1. https://nvd.nist.gov/vuln/detail/cve-2026-58868
2. https://source.android.com/docs/security/bulletin/2026/2026-11-01
3. https://thehackernews.com/2026/11/google-patches-critical-android-flaw.html

ข้อมูลอ้างอิง OpenSSH

1. https://nvd.nist.gov/vuln/detail/cve-2026-123158
2. https://www.openssh.org/releasenotes.html#10.6p2
3. https://www.securityweek.com/openssh-rushes-patches-for-sshole-authentication-bypass

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ

แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ

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

TLP Color : CLEAR



ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

ช่องโหว่ในผลิตภัณฑ์ Google, OpenSSH (Sshole) และ SonicWall เสี่ยงถูกใช้ในการโจมตี

วันที่แจ้งเตือน 10 พฤศจิกายน 2569

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
SonicWall	• **ช่องโหว่ CVE-2026-109593** ใน Global Management System (GMS) ซึ่ง End-of-Life (EOL) แล้ว ส่งผลให้ผู้ไม่หวังดีที่สามารถเข้าถึงระบบผ่านเครือข่าย สามารถอ่านไฟล์ภายในระบบและขโมยข้อมูลสำคัญได้ โดยไม่ต้องผ่านการยืนยันตัวตน (Unauthenticated) • **ช่องโหว่ CVE-2026-109594** เป็นช่องโหว่ประเภท SQL Injection ใน Sonicwall GMS ซึ่งผู้ไม่หวังดีที่ผ่านการตรวจสอบสิทธิสามารถใช้ประโยชน์จากช่องโหว่ แทรกคำสั่ง SQL เพื่อเข้าถึงหรือแก้ไขข้อมูลที่จัดเก็บอยู่ใน Database ของระบบได้	• ส่งผลกระทบต่อผลิตภัณฑ์ SonicWall GMS - Virtual Appliance and Windows เวอร์ชัน 9.5.2 และเวอร์ชันก่อนหน้า • แนะนำให้ผู้ใช้งาน SonicWall GMS เวอร์ชัน 9.5.2 หรือก่อนหน้า พิจารณาอัปเกรดไปใช้ SonicWall Network Security Manager (NSM) ตามคำแนะนำของผู้ผลิต
	• **ช่องโหว่ CVE-2026-19868** เป็นช่องโหว่ประเภท Authentication Bypass ในระบบปฏิบัติการ SonicOS ในบริการ SSLVPN เกิดขึ้นในขั้นตอนกระบวนการยืนยันตัวตนผ่าน Security Assertion Markup Language Authentication (“SAML”) ทำให้ผู้ไม่หวังดีที่มี Credential สามารถใช้ประโยชน์จากช่องโหว่ดังกล่าว โดยข้ามกระบวนการตรวจสอบ SAML และ MFA ได้	• ส่งผลกระทบต่อผลิตภัณฑ์ Sonic OS - 7.3.3-7015 และเวอร์ชันก่อนหน้า - 8.2.2-8015 และเวอร์ชันก่อนหน้า • เวอร์ชันที่แก้ไขช่องโหว่แล้ว ได้แก่ SonicOS 7.3.4-7013 หรือใหม่กว่าสำหรับ Gen7 และ SonicOS 8.2.3-8015 หรือใหม่กว่าสำหรับ Gen8

ข้อมูลอ้างอิง SonicWall

1. https://nvd.nist.gov/vuln/detail/cve-2026-109593
2. https://nvd.nist.gov/vuln/detail/cve-2026-109594
3. https://nvd.nist.gov/vuln/detail/cve-2026-19868
4. https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0019
5. https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0014
6. https://www.bleepingcomputer.com/news/security/sonicwall-warns-of-unpatched-flaws-in-end-of-life-gms-software/
7. https://cybersecuritynews.com/sonicos-sslvpn-vulnerability-exploited/