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 TeamViewer และ Juniper Network เสี่ยงถูกใช้ในการโจมตี

วันที่แจ้งเตือน 6 พฤศจิกายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า ช่องโหว่ในผลิตภัณฑ์ TeamViewer, Juniper และช่องโหว่ใน Node.js ที่อาจถูกนำไปใช้ในการโจมตีและทำให้เกิดความเสี่ยงต่อระบบสารสนเทศขององค์กร ได้แก่

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Team Viewer	• ช่องโหว่ **CVE-2026-111585** เป็นช่องโหว่ประเภท Integer Overflow ของ TeamViewer เกิดจากกระบวนการคำนวณขนาดหน่วยความจำไม่ถูกต้องในขั้นตอนการประมวลผล Screen Decompression ทำให้ผู้ไม่หวังดีใช้อุปกรณ์ปลายทางที่ถูกควบคุม ส่งข้อมูลหน้าจอที่สร้างขึ้นไปยังเครื่องของผู้ใช้งานที่กำลังเชื่อมต่อผ่าน TeamViewer ทำให้เกิดการทำงานผิดพลาดหรือหยุดให้บริการได้ • ช่องโหว่ **CVE-2026-92372** เป็นช่องโหว่ประเภท Out-of-Bounds Write เกิดจากการตรวจสอบขอบเขตหน่วยความจำที่ไม่ถูกต้องในขั้นตอน Screen-Image Decoder บนระบบปฏิบัติการ Linux และ macOS ทำให้ผู้ไม่หวังดีสามารถส่งข้อมูลภาพหน้าจอที่ถูกปรับแต่งระหว่างการเชื่อมต่อระยะไกลหรือหลอกลวงให้ผู้ใช้งานเปิดไฟล์บันทึก Session TeamViewer ที่สร้างขึ้น เพื่อควบคุมเครื่องคอมพิวเตอร์ของผู้ใช้งานได้ • ช่องโหว่ **CVE-2026-92374** เป็นช่องโหว่ประเภท Time-of-check Time-of-use (TOCTOU) เกิดจากความผิดพลาดในขั้นตอนการตรวจสอบแพ็กเกจติดตั้งและขั้นตอนการนำแพ็กเกจไปใช้งานบนระบบปฏิบัติการ macOS ทำให้ผู้ไม่หวังดีสามารถข้ามกระบวนการตรวจสอบแพ็กเกจและยกระดับสิทธิเป็น Root เข้าควบคุมเครื่องคอมพิวเตอร์ได้ • บริษัทผู้ผลิตแนะนำให้ผู้ใช้ผลิตภัณฑ์ดังกล่าว ดำเนินการอัปเกรดเป็นซอฟต์แวร์เวอร์ชัน 15.83 หรือเวอร์ชันล่าสุด	• TeamViewer Full Client, Host และ Portable เวอร์ชันต่ำกว่า 15.83 (รวมถึง Legacy/Maintenance เช่น v15.64 บน Windows 7/8, v13.2 บน Windows, Linux และ macOS เป็นต้น • TeamViewer Remote Control App (บน Android) เวอร์ชันต่ำกว่า 15.83

ข้อมูลอ้างอิง Microsoft

1. https://nvd.nist.gov/vuln/detail/cve-2026-111585
2. https://nvd.nist.gov/vuln/detail/cve-2026-92372
3. https://nvd.nist.gov/vuln/detail/cve-2026-92374
4. https://www.teamviewer.com/en/resources/trust-center/security-bulletins/tv-2026-1011/
5. https://thehackernews.com/2026/10/teamviewer-flaw-lets-remote-computers.html

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 TeamViewer และ Juniper Network เสี่ยงถูกใช้ในการโจมตี

วันที่แจ้งเตือน 6 พฤศจิกายน 2569

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Juniper Network	• **ช่องโหว่ CVE-2026-103406** เป็นช่องโหว่ใน Session Smart Conductor ของกระบวนการจัดการ Key ทำให้ผู้ไม่หวังดีสั่งรันคำสั่งบนอุปกรณ์ได้โดยไม่ต้องผ่านกระบวนการยืนยันตัวตน • **ช่องโหว่ CVE-2026-103409** เป็นช่องโหว่ใน Session Smart Router ทำให้ผู้ไม่หวังดีได้รับสิทธิระดับ Admin โดยไม่ต้องผ่านการยืนยันตัวตน จากนั้นสามารถเข้าสู่ระบบทำการแก้ไขข้อมูลหรือการตั้งค่าของระบบได้ • **Juniper Network** แนะนำให้ผู้ใช้ผลิตภัณฑ์ดังกล่าว ดำเนินการอัปเกรดเป็นซอฟต์แวร์เวอร์ชันแก้ไขที่ระบุไว้แล้วหรือใหม่กว่า	ส่งผลกระทบต่อผลิตภัณฑ์ Session Smart Router and Session Smart Conductor - เวอร์ชันต่ำกว่า 7.0.5 - เวอร์ชันต่ำกว่า 7.1.7 - เวอร์ชันต่ำกว่า 7.2.3 • ซอฟต์แวร์เวอร์ชันแก้ไข 7.0.5, 7.1.7 และ 7.2.3

ข้อมูลอ้างอิง Juniper Network

1. https://nvd.nist.gov/vuln/detail/cve-2026-103406
2. https://nvd.nist.gov/vuln/detail/cve-2026-103409
3. https://supportportal.juniper.net/JSA112183
4. https://www.securityweek.com/adobe-veeam-juniper-networks-patch-critical-vulnerabilities/

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

Node.js ได้ออกแพตช์ความปลอดภัยเพื่อแก้ไขช่องโหว่

วันที่แจ้งเตือน 6 พฤศจิกายน 2569

รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
1. **ช่องโหว่ CVE-2026-105482** เป็นช่องโหว่ในการตรวจสอบชื่อโดเมนผ่าน DNS เมื่อชื่อโดเมนมีอักขระพิเศษ NUL อาจทำให้ระบบตรวจสอบปลายทางผิดพลาดและหลีกเลี่ยงข้อจำกัดการเข้าถึงได้ 2. **ช่องโหว่ CVE-2026-105483** เป็นช่องโหว่ในการตรวจสอบ Hostname ของ TLS เมื่อใช้หมายเลข IP ที่มีตัวเลข Unicode แบบ Fullwidth Digits อาจทำให้ระบบยอมรับใบรับรองที่ไม่ตรงกับหมายเลข IP ของ Server ปลายทาง 3. **ช่องโหว่ CVE-2026-106069** เป็นช่องโหว่ในการตรวจสอบ Hostname ของ TLS เมื่อใช้หมายเลข IP ในรูปแบบที่ไม่เป็นมาตรฐาน อาจทำให้ระบบตรวจสอบใบรับรองกับหมายเลข IP ที่แตกต่างจากปลายทางที่เชื่อมต่อจริง ส่งผลให้เกิดความเสี่ยงจากการปลอมแปลงตัวตนของ Server 4. **ช่องโหว่ CVE-2026-111497 (Node2Shell)** เป็นช่องโหว่ประเภท Out-of-Bounds Write ในส่วนการถอดรหัสข้อมูลบีบอัด (Brotli Decoder) ซึ่งทำให้ผู้ไม่หวังดีสามารถส่งข้อมูลที่สร้างขึ้นไปยังแอปพลิเคชันที่มีการถอดรหัส Brotli ทำให้หน่วยความจำเสียหาย ระบบหยุดทำงาน ข้อมูลรั่วไหลหรือผู้ไม่หวังดีสั่งรันโค้ดอันตรายบน Server เป้าหมายได้จากระยะไกล (RCE)	Node.js ได้เผยแพร่เวอร์ชันแก้ไขช่องโหว่แล้วเมื่อวันที่ 21 ตุลาคม 2569 โดยผู้ดูแลระบบต้องดำเนินการอัปเดต Node.js เป็นเวอร์ชันล่าสุดที่ได้รับการแก้ไขแล้ว ได้แก่ • ผู้ใช้งานเวอร์ชัน 26.x ให้อัปเดตเป็นเวอร์ชัน 26.12.1 หรือใหม่กว่า • ผู้ใช้งานเวอร์ชัน 24.x ให้อัปเดตเป็นเวอร์ชัน 24.22.1 หรือใหม่กว่า • ผู้ใช้งานเวอร์ชัน 22.x ให้อัปเดตเป็นเวอร์ชัน 22.23.4 หรือใหม่กว่า ทั้งนี้ สำหรับ Node.js เวอร์ชันที่ End of Life ควรพิจารณาใช้เวอร์ชันปัจจุบันที่ได้รับการอัปเดตด้านความมั่นคงปลอดภัย โดยดาวน์โหลดได้ที่ https://nodejs.org/en/download

แนวทางการตรวจสอบและป้องกันความเสี่ยง

- ตรวจสอบระบบที่ใช้งาน Node.js ทั้งบนเว็บเซิร์ฟเวอร์ แอปพลิเคชัน และ Container เพื่อระบุระบบและเวอร์ชันที่อาจได้รับผลกระทบ
- อัปเดต Node.js เป็นเวอร์ชันที่ได้รับการแก้ไข พร้อมทดสอบระบบหลังอัปเดต และตรวจสอบแอปพลิเคชัน/API ที่รับข้อมูลภายนอก โดยเฉพาะส่วนที่เกี่ยวข้องกับ Brotli, HTTPS และการตรวจสอบชื่อโดเมน
- เฝ้าระวังและตรวจสอบ Logs เพื่อค้นหาความผิดปกติ จำกัดบริการที่เปิดสู่ Internet เท่าที่จำเป็น

ข้อมูลอ้างอิง Node.js

1. https://nvd.nist.gov/vuln/detail/CVE-2026-105482
2. https://nvd.nist.gov/vuln/detail/CVE-2026-105483
3. https://nvd.nist.gov/vuln/detail/CVE-2026-106069
4. https://nvd.nist.gov/vuln/detail/CVE-2026-111497
5. https://github.com/nodejs/Release#release-schedule
6. https://nodejs.org/en/blog/vulnerability/october-2026-security-releases
7. https://cybersecuritynews.com/node-js-schedules-patch/