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 NGINX

CVE-2026-15176, CVE-2026-97205 และ CVE-2026-93479

วันที่แจ้งเตือน 27 ตุลาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ThaiCERT สกมช. ได้ติดตามสถานการณ์ภัยคุกคามทางไซเบอร์พบรายงานกรณีช่องโหว่ในผลิตภัณฑ์ NGINX จำนวน 3 รายการ ส่งผลให้ผู้ไม่หวังดีอาจสามารถส่ง HTTP Request เพื่อทำให้ NGINX จัดการหน่วยความจำผิดพลาด หรือหยุดทำงาน (Denial-of-Service : DoS) หรืออาจนำไปสู่การรันคำสั่งที่เป็นอันตรายบนระบบได้

การโจมตี

- CVE-2026-15176 เป็นช่องโหว่ประเภท Heap-based Buffer Overflow ผู้ไม่หวังดีอาจส่งข้อมูลที่ทำให้ NGINX จัดการหน่วยความจำผิดพลาด ส่งผลให้โปรแกรมหยุดทำงานหรือ restart หรืออาจนำไปสู่การรันโค้ดของผู้โจมตี
- CVE-2026-93479 เป็นช่องโหว่ประเภท Heap-based Buffer Overflow ในส่วนที่ NGINX เมื่อใช้คำสั่ง map ร่วมกับการประมวลผลสตริง และ Regular Expression (Regex) ซึ่งการอ้างอิงตัวแปรใน configuration ไม่ถูกต้องและทำให้จัดการหน่วยความจำผิดพลาด
- CVE-2026-97205 เป็นช่องโหว่ประเภท Use-After-Free (UAF) เกี่ยวข้องกับปัญหาการจัดการหน่วยความจำ ซึ่งอาจทำให้ NGINX worker process ล่ม หรือ restart และมีโอกาสนำไปสู่ code execution

ช่องโหว่ ⟶ NGINX จัดการข้อมูล/หน่วยความจำผิดพลาด ⟶ Worker Process อาจล่มหรือ Restart ⟶ บางเงื่อนไขอาจพัฒนาไปถึง Code Execution

ผลกระทบ

ผลิตภัณฑ์ที่ได้รับผลกระทบ:

ผลิตภัณฑ์	เวอร์ชันที่ได้รับผลกระทบ	เวอร์ชันที่แนะนำให้อัปเดต
NGINX Open Source	ก่อน 1.30.6 และ 1.31.7	1.30.6 หรือ 1.31.7 ขึ้นไป
NGINX Plus 37.x	37.0.0–37.0.4 และ 37.1.0	37.0.5.1 หรือ 37.1.0.1 ขึ้นไป
NGINX Plus R33–R36	ได้รับผลกระทบและไม่มี Fix ใน Branch เดิม	ย้ายไปยัง Branch ที่มี Security Fix
NGINX Instance Manager	2.18.0–2.23.0	2.24.0 ขึ้นไป
F5 WAF for NGINX	5.9.0–5.15.0 ตาม Branch ที่เกี่ยวข้อง	5.16.0 หรือ 5.14.2
F5 DoS for NGINX	4.8.0–4.10.0	4.11.0 ขึ้นไป
NGINX Gateway Fabric	2.1.0–2.7.2	2.8.0 ขึ้นไป
NGINX Ingress Controller	5.6.0–5.6.3	5.7.0 ขึ้นไป

คำแนะนำ: ผู้ใช้งานและผู้ดูแลระบบที่ใช้ผลิตภัณฑ์ F5 NGINX ที่ได้รับผลกระทบควรอัปเดตเป็นเวอร์ชันล่าสุดที่มีการแก้ไขด้านความปลอดภัยโดยทันที ในกรณีที่ยังไม่สามารถติดตั้งแพตช์หรืออัปเดตได้ทันที ผู้ดูแลระบบควรพิจารณาใช้มาตรการบรรเทาความเสี่ยงชั่วคราวดังต่อไปนี้

- CVE-2026-15176: หลีกเลี่ยงการใช้คำสั่ง alias ภายใน location block หรือหลีกเลี่ยงการใช้ตัวแปร $request_filename
- CVE-2026-97205: ปิดการใช้งาน Asynchronous File I/O (AIO) หรือ Server Side Includes (SSI)
- CVE-2026-93479: ใช้ Named Captures แทน Unnamed Captures และจำกัดการใช้งาน Named Captures ให้อยู่เฉพาะภายใน configuration block ที่มีการจับคู่ด้วย Regular Expression (Regex) นั้น

คำแนะนำด้านความปลอดภัยเพิ่มเติม:

1. เฝ้าระวังและตรวจสอบ Log โดยเฉพาะ Access Log และ Error Log เพื่อค้นหา HTTP Request ที่ผิดปกติ รวมถึงเหตุการณ์ Worker Process หยุดทำงาน หรือ Restart โดยไม่ทราบสาเหตุ
2. ตรวจสอบพฤติกรรมผิดปกติของระบบ เช่น การสร้าง Process ที่ไม่คาดคิด การเชื่อมต่อไปยัง IPภายนอกที่น่าสงสัย หรือการเปลี่ยนแปลงไฟล์สำคัญโดยไม่ได้รับอนุญาต
3. เสริมมาตรการป้องกันระดับระบบปฏิบัติการ โดยเปิดใช้งาน ASLR และมาตรการป้องกันการโจมตีหน่วยความจำ เพื่อลดความเสี่ยงจากการนำช่องโหว่ไปใช้รันโค้ดอันตราย
4. เตรียมความพร้อมในการรับมือเหตุการณ์ หากพบหลักฐานการโจมตีหรือการบุกรุกระบบ ควรจำกัดการเข้าถึงระบบที่ได้รับผลกระทบ เก็บรักษาหลักฐาน และดำเนินการตามกระบวนการ Incident Response

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 26 ต.ค. 2569
2. https://www.bleepingcomputer.com/news/security/f5-releases-out-of-band-patches-for-critical-nginx-vulnerabilities/?
3. https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2026-150/

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

ช่องโหว่ Critical ในผลิตภัณฑ์ Next.js

วันที่แจ้งเตือน 27 ตุลาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ThaiCERT สกมช. ได้ติดตามสถานการณ์ภัยคุกคามทางไซเบอร์พบรายงานกรณีช่องโหว่ระดับ Critical จำนวน 2 รายการ ใน Next.js (Web Framework สำหรับพัฒนาเว็บแอปพลิเคชัน) เสี่ยงถูกสั่งรันคำสั่ง (Remote Code Execution: RCE) รวมถึงช่องโหว่ระดับสูง 1 รายการที่อาจทำให้ระบบหยุดให้บริการ (Denial of Service: DoS) ได้

การโจมตี	ผลกระทบ
1. Remote Code Execution ผ่าน use cache **(Critical)** กระทบแอปพลิเคชันที่ใช้ App Router + Cache Components หากฟังก์ชัน use cache คืนค่า typed arrays หลายรายการ อาจนำไปสู่ Remote Code Execution โดย Next.js แนะนำให้อัปเกรดทันที แม้แอปพลิเคชันจะไม่ได้มีฟังก์ชันลักษณะดังกล่าวก็ตาม 2. Remote Code Execution ผ่าน Image Optimization เมื่อใช้ SVG **(Critical)** CVE-2026-96889 เป็นช่องโหว่เกี่ยวกับหน่วยความจำใน upstream library ที่ Next.js ใช้สำหรับ Image Optimization ซึ่งอาจนำไปสู่ Remote Code Execution เมื่อ Next.js ทำงานบน Linux ที่ใช้ glibc 3. ช่องโหว่ Denial of Service ผ่าน Server Actions **(High)** กระทบแอปพลิเคชันที่ใช้ App Router และมี Server Action อย่างน้อยหนึ่งรายการ ผู้ไม่หวังดีสามารถส่ง crafted request เพื่อทำให้เกิด CPU usage สูงผิดปกติ ส่งผลให้ process ไม่สามารถประมวลผล request อื่นต่อได้ แอปพลิเคชันที่ใช้ Pages Router หรือ ไม่ได้ใช้ Server Actions ไม่ได้รับผลกระทบจากช่องโหว่นี้	**ผลิตภัณฑ์ที่ได้รับผลกระทบ:** 1.ช่องโหว่ RCE ผ่าน use cache (Critical) Next.js เวอร์ชัน 16.0.0 ถึง 16.4.0 2. ช่องโหว่ RCE ผ่าน Image Optimization เมื่อใช้ SVG (Critical) Next.js เวอร์ชัน 10.0.0 ถึง 15.5.27 Next.js เวอร์ชัน 16.0.0 ถึง 16.4.0 3. ช่องโหว่ Denial of Service ผ่าน Server Actions (High) Next.js เวอร์ชัน 13.0.0 ถึง 15.5.27 Next.js เวอร์ชัน 16.0.0 ถึง 16.4.0 **ผลกระทบที่อาจเกิดขึ้น:** • ช่องโหว่ RCE ผู้ไม่หวังดีอาจสามารถเข้าถึงหรือแก้ไขข้อมูลสำคัญ ติดตั้งมัลแวร์ หรือ Backdoor รวมถึงใช้ระบบที่ถูกเจาะเป็นจุดเริ่มต้นในการโจมตีระบบอื่น • ช่องโหว่ Denial of Service ผู้ไม่หวังดีอาจส่งคำขอที่สร้างขึ้นส่งผลให้ CPU ของเซิร์ฟเวอร์ทำงานสูงผิดปกติ ส่งผลให้เว็บแอปพลิเคชันตอบสนองช้าหรือไม่สามารถให้บริการแก่ผู้ใช้งานได้

แนวทางการตรวจสอบและป้องกัน:

1. ตรวจสอบเวอร์ชัน Next.js ของเว็บแอปพลิเคชันและระบบ Production ทั้งหมด โดยเฉพาะระบบที่สามารถเข้าถึงได้จากอินเทอร์เน็ต
2. ผู้ใช้งาน Next.js 16 ควรพิจารณาอัปเดตเป็น Next.js 16.4.1 หรือใหม่กว่า โดยเร็วที่สุด
3. ผู้ใช้งาน Next.js 15 ควรพิจารณาอัปเดตเป็น Next.js 15.5.28 หรือใหม่กว่า และดำเนินการ Build และ Deploy แอปพลิเคชันใหม่หลังการอัปเดต
4. สำหรับ Next.js 15 ให้ตรวจสอบเวอร์ชันของ sharp ด้วยคำสั่ง ‘npm ls sharp’ และตรวจสอบให้แน่ใจว่าเป็นเวอร์ชัน 0.35.5 ขึ้นไป เนื่องจากการอัปเกรด Next.js บนระบบเดิมอาจยังคงมี sharp เวอร์ชันเก่าติดตั้งอยู่
5. ตรวจสอบ Logs ของ Web Server, Application Server, WAF และระบบ SIEM เพื่อค้นหาคำขอที่ผิดปกติ การใช้ทรัพยากร CPU สูงผิดปกติ รวมถึงกิจกรรมต้องสงสัยที่เกี่ยวข้องกับการอัปโหลดหรือประมวลผลไฟล์ SVG

แนวทางลดความเสี่ยงชั่วคราว:

1. หากยังไม่สามารถอัปเดต Next.js ได้ทันที สำหรับช่องโหว่ CVE-2026-96889 ให้ดำเนินการอัปเดต sharp เป็นเวอร์ชัน 0.35.5 ขึ้นไป
2. หลีกเลี่ยงหรือปิดการประมวลผลไฟล์ SVG จากแหล่งที่ไม่น่าเชื่อถือ และตรวจสอบการตั้งค่า ‘dangerouslyAllowSVG’ หากไม่มีความจำเป็นควรปิดใช้งาน
3. จำกัดประเภทและขนาดของไฟล์ที่ผู้ใช้งานสามารถอัปโหลดเข้าสู่ระบบ พร้อมตรวจสอบความถูกต้องของไฟล์ก่อนเข้าสู่กระบวนการ Image Optimization
4. สำหรับช่องโหว่ 'use cache' และ Server Actions ปัจจุบันไม่มีแนวทางแก้ไขชั่วคราวที่สามารถป้องกันช่องโหว่ได้อย่างสมบูรณ์ จึงควรดำเนินการอัปเดตเป็นเวอร์ชันที่ได้รับการแก้ไขโดยเร็วที่สุด

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 26 ต.ค. 2569
2. https://nextjs.org/blog/nextjs-security-update-october-14-2026