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 GitLab, Fortinet และ Microsoft Authenticator เสี่ยงถูกใช้ในการโจมตี

วันที่แจ้งเตือน 28 ตุลาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ThaiCERT สกมช. ได้ติดตามสถานการณ์ภัยคุกคามทางไซเบอร์ พบรายงานกรณีช่องโหว่ด้านความมั่นคงปลอดภัยระดับ Critical ใน GitLab ซึ่งเป็นแพลตฟอร์มสำหรับจัดการซอร์สโค้ดและกระบวนการพัฒนาซอฟต์แวร์ ซึ่งผู้ไม่หวังดีอาจใช้ประโยชน์จากช่องโหว่ดังกล่าวโดยสั่งรันคำสั่งบนเซิร์ฟเวอร์ Remote Code Execution: RCE และแก้ไข Source Code รวมถึงการติดตั้ง มัลแวร์ หรือ Backdoor ทำให้เกิดผลกระทบต่อระบบขององค์กรได้

การโจมตี

- CVE-2026-110264 เป็นช่องโหว่ประเภท Integer Overflow ในตัวคอมไพเลอร์ Regular Expression ของเอนจิน Onigmo ซึ่งเป็นไลบรารีจัดการ Regex ที่ถูกบิวด์อินอยู่ในภาษา Ruby และส่งผลกระทบโดยตรงต่อระบบ GitLab CE/EE เวอร์ชัน Self-managed

ผลกระทบที่อาจเกิดขึ้น:

- ผู้ไม่หวังดีอาจสามารถสั่งรันคำสั่งอันตรายบนเซิร์ฟเวอร์ GitLab โดยข้ามกระบวนการยืนยันตัวตน ภายใต้เงื่อนไขที่ทำให้ช่องโหว่สามารถถูกโจมตีได้
- หากโจมตีสำเร็จ อาจส่งผลให้ผู้โจมตีเข้าถึงหรือแก้ไข Source Code และข้อมูลสำคัญที่จัดเก็บอยู่ในระบบ รวมถึงอาจนำไปสู่การติดตั้งมัลแวร์หรือ Backdoor
- ระบบ GitLab ที่ถูกบุกรุกอาจถูกใช้เป็นจุดเริ่มต้นในการโจมตีระบบอื่นที่เชื่อมต่อกัน เช่น ระบบ CVCD หรือโครงสร้างพื้นฐานสำหรับพัฒนาและเผยแพร่ซอฟต์แวร์ เป็นต้น

ผลกระทบ

ผลิตภัณฑ์ที่ได้รับผลกระทบ: ช่องโหว่นี้กระทบ GitLab Self-managed ตั้งแต่ version 7.0 ซึ่งออกในปี 2014 ไปจนถึงรุ่นปัจจุบันที่ยังไม่ได้ patch

Affected Version	Upgraded Version
GitLab 19.5 ก่อน Version 19.5.1	19.5.1
GitLab 19.4 ก่อน Version 19.4.3	19.4.3
GitLab 19.3 ก่อน Version 19.3.6	19.3.6
GitLab 19.2 ก่อน Version 19.2.9	19.2.9
GitLab 19.1 ก่อน Version 19.1.9	19.1.9
GitLab 19.0 ก่อน Version 19.0.10	19.0.10
GitLab 7.0 - 18.11 (ก่อน Version 18.11.13)	18.11.13

แนวทางการตรวจสอบและป้องกัน:

- ตรวจสอบเวอร์ชัน GitLab Self-Managed ที่ใช้งานทั้งหมด โดยเฉพาะเซิร์ฟเวอร์ที่เปิดให้เข้าถึงจากอินเทอร์เน็ต
- พิจารณาอัปเดต GitLab เป็นเวอร์ชันใหม่กว่าที่มีการแก้ไขช่องโหว่แล้ว
- ตรวจสอบ Application Logs และ System Logs เพื่อค้นหาความผิดปกติ โดยเฉพาะ Worker Process หรือข้อผิดพลาดที่เกี่ยวข้องกับ Regular Expression
- ใช้ Detection Rules เพื่อช่วยตรวจสอบพฤติกรรมที่อาจเกี่ยวข้องกับการโจมตีของ GitLab ได้แก่ Onigmo native worker crash และ Org mode render error burst ผ่านเครื่องมือ TLDR Framework หรือปรับใช้กับระบบ SIEM
- สำรองข้อมูลและวางแผนการอัปเดตก่อนดำเนินการ โดยเฉพาะ GitLab 19.3.6 และ 19.4.3 จะมีการเปลี่ยนแปลงฐานข้อมูลระหว่างการอัปเกรดและอาจทำให้ระบบแบบ Single-Node หยุดให้บริการชั่วคราว

แนวทางลดความเสี่ยงชั่วคราว:

1. จำกัดการเข้าถึง GitLab จากอินเทอร์เน็ต โดยอนุญาตเฉพาะเครือข่ายหรือผู้ใช้งานที่จำเป็นผ่าน VPN หรือ Firewall
2. เพิ่มการเฝ้าระวัง Logs และแจ้งเตือนเมื่อพบการทำงานผิดปกติของ GitLab โดยเฉพาะ Worker Crash หรือข้อผิดพลาดที่เกิดขึ้นซ้ำจำนวนมาก
3. ตรวจสอบสิทธิการเข้าถึงระบบและจำกัดสิทธิของบัญชีบริการ (Service Account) รวมถึงข้อมูลรับรองที่ GitLab ใช้เชื่อมต่อกับระบบอื่น

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 28 ต.ค. 2569
2. https://thehackernews.com/2026/10/critical-gitlab-flaw-cvss-100-could.html?

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 GitLab, Fortinet และ Microsoft Authenticator เสี่ยงถูกใช้ในการโจมตี

วันที่แจ้งเตือน 28 ตุลาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบช่องโหว่ในผลิตภัณฑ์ Fortinet FortiSIEM เสี่ยงถูกนำไปใช้ในการโจมตีระบบสารสนเทศขององค์กร

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Fortinet	• **ช่องโหว่ CVE-2026-106173** เป็นช่องโหว่ประเภท Path Traversal ในผลิตภัณฑ์ Fortinet FortiSIEM เกิดจากการทำงานในส่วนประมวลผลคำขอ QueryResultReq ของบริการ gRPC ใน FortiSIEM ที่มีการจัดการข้อมูลที่ได้รับจากภายนอกโดยไม่ได้ตรวจสอบเส้นทางไฟล์อย่างเหมาะสม ส่งผลให้ผู้ไม่หวังดีอาจใช้ประโยชน์จากช่องโหว่ดังกล่าวสั่งรันโค้ดหรือคำสั่งบนระบบผ่านการส่งแพ็กเก็ตข้อมูลที่ถูกสร้างขึ้นมาเป็นพิเศษ โดยไม่จำเป็นต้องผ่านขั้นตอนการยืนยันตัวตน • **Fortinet** แนะนำให้ผู้ใช้ผลิตภัณฑ์ดังกล่าว ดำเนินการอัปเกรดเป็นซอฟต์แวร์เวอร์ชันแก้ไขที่ระบุไว้แล้ว	ส่งผลกระทบต่อ ผลิตภัณฑ์ - FortiSIEM เวอร์ชัน 7.5.0 - FortiSIEM เวอร์ชัน 7.4.0 - 7.4.2 - FortiSIEM เวอร์ชัน 7.3.0 - 7.3.5 - FortiSIEM เวอร์ชัน 7.2.0 - 7.2.7 - FortiSIEM เวอร์ชัน 7.1.0 - 7.1.9 - FortiSIEM เวอร์ชัน 7.0.0 - 7.0.4 • ซอฟต์แวร์เวอร์ชันแก้ไข FortiSIEM 7.5.1

ข้อมูลอ้างอิง Fortinet

1. https://nvd.nist.gov/vuln/detail/cve-2026-106173
2. https://fortiguard.fortinet.com/psirt/FG-IR-26-180
3. https://thehackernews.com/2026/10/critical-fortisiem-flaw-gets-public.html?

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 GitLab, Fortinet และ Microsoft Authenticator เสี่ยงถูกใช้ในการโจมตี

วันที่แจ้งเตือน 28 ตุลาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า ช่องโหว่ในผลิตภัณฑ์ Microsoft Authenticator สำหรับ Android เสี่ยงถูกนำไปใช้ในการโจมตีระบบสารสนเทศขององค์กร

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Microsoft	• ช่องโหว่ **CVE-2026-80097** ในแอปพลิเคชัน Microsoft Authenticator สำหรับ Android เกิดจากขั้นตอนการตรวจสอบตัวตนของแอปพลิเคชันที่ร้องขอ Token ไม่ถูกต้อง ซึ่งผู้ไม่หวังดีอาจใช้ประโยชน์จากช่องโหว่ดังกล่าวโดยใช้แอปพลิเคชันอื่นบนเครื่อง Andriod สวมรอยเป็นแอปพลิเคชันที่ได้รับอนุญาต (เช่น Microsoft Teams) และขโมย Access Token ไปได้ ทำให้ผู้ไม่หวังดีเข้าถึงอีเมล ไฟล์ หรือข้อมูลสำคัญได้ • Microsoft แนะนำให้ผู้ใช้ผลิตภัณฑ์ดังกล่าว ดำเนินการอัปเกรดเป็นซอฟต์แวร์เวอร์ชันแก้ไขที่ระบุไว้แล้ว	• ส่งผลกระทบต่อผลิตภัณฑ์ Microsoft Authenticator for Android เวอร์ชั่นที่ต่ำกว่า 6.2606.4246 • ซอฟต์แวร์เวอร์ชันแก้ไข 6.2606.4246

ข้อมูลอ้างอิง Microsoft

1. https://nvd.nist.gov/vuln/detail/cve-2026-80097
2. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-80097
3. https://cybersecuritynews.com/microsoft-authenticator-flaw/

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ