เอกสารแจ้งเตือนกรณีช่องโหว่ Vite Development Server ถูกใช้โจมตี อาจเสี่ยงเปิดเผยข้อมูลสำคัญ

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เกี่ยวกับกรณีช่องโหว่ Vite Development Server ถูกใช้โจมตี อาจเสี่ยงเปิดเผยข้อมูลสำคัญ

พบรายงานการใช้ประโยชน์จากช่องโหว่ใน Vite Development Server ซึ่งเป็นเครื่องมือสำหรับพัฒนาเว็บไซต์และแอปพลิเคชัน โดยผู้ไม่หวังดีสามารถใช้ช่องโหว่ดังกล่าว เพื่อเข้าถึงไฟล์ภายในระบบที่ไม่ได้รับอนุญาต ส่งผลให้ข้อมูลสำคัญ เช่น ไฟล์ตั้งค่าระบบ ข้อมูลยืนยันตัวตน (Credentials) หรือข้อมูลสำหรับเชื่อมต่อบริการต่าง ๆ อาจถูกเปิดเผย และถูกนำไปใช้เพื่อโจมตีระบบเพิ่มเติมได้[1]

จากรายงานของ F5 Labs พบการตรวจพบการสแกนระบบที่เปิดใช้งาน Vite Development Server ผ่านอินเทอร์เน็ต และมีความพยายามใช้ประโยชน์จากช่องโหว่ CVE-2026-39364 เพื่อเข้าถึงไฟล์สำคัญภายในระบบ เช่น ไฟล์กำหนดค่า ระบบคลาวด์ และข้อมูล Credentials ซึ่งอาจเพิ่มความเสี่ยงต่อการเข้าถึงภายในหน่วยงานโดยไม่ได้รับอนุญาต[2]

<u>รายละเอียดช่องโหว่</u>

CVE-2026-39364 (CVSS v3.1: 7.5)[3] เป็นช่องโหว่ประเภท Information Disclosure (การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต) ใน Vite Development Server ช่องโหว่ดังกล่าวเกิดจากการตรวจสอบสิทธิ์การเข้าถึงไฟล์ภายในระบบไม่เพียงพอ ทำให้ผู้โจมตีสามารถส่งคำร้องขอจากภายนอกเพื่อเข้าถึงไฟล์ที่ควรถูกจำกัดได้ โดยไม่จำเป็นต้องมีบัญชีผู้ใช้งานหรือสิทธิ์พิเศษ ข้อมูลที่อาจถูกเปิดเผย ได้แก่

- ไฟล์ตั้งค่าระบบ (Configuration Files)
- ข้อมูลยืนยันตัวตน (Credentials)
- API Key หรือ Token
- ข้อมูลเชื่อมต่อกับบริการภายนอก

ข้อมูลดังกล่าวอาจถูกนำไปใช้เพื่อเข้าถึงระบบอื่น หรือขยายผลการโจมตีภายในหน่วยงานเพิ่มเติม

<u>รูปแบบการโจมตีและผลกระทบ</u>

ผู้โจมตีอาจดำเนินการโดยค้นหาระบบ Vite Development Server ที่เปิดให้บริการผ่านอินเทอร์เน็ต จากนั้นใช้ช่องโหว่ CVE-2026-39364 เพื่อเข้าถึงไฟล์ภายในระบบที่ไม่ได้รับอนุญาต หากการโจมตีสำเร็จอาจส่งผลกระทบ ดังนี้

1. การเปิดเผยข้อมูลสำคัญของหน่วยงาน โดยผู้โจมตีอาจเข้าถึงข้อมูล เช่น ไฟล์ตั้งค่าระบบ ข้อมูลบัญชีผู้ใช้งาน Credentials, Token หรือข้อมูลเชื่อมต่อบริการต่าง ๆ ซึ่งอาจถูกนำไปใช้โดยไม่ได้รับอนุญาต

2. การเข้าถึงระบบหรือบริการอื่นเพิ่มเติม ซึ่งข้อมูล Credentials หรือ Token ที่ถูกเปิดเผย อาจถูกนำไปใช้เพื่อเข้าถึงระบบภายใน ระบบคลาวด์ หรือบริการอื่นที่เกี่ยวข้อง ส่งผลให้ผู้โจมตีสามารถขยายขอบเขตการเข้าถึงได้
3. การเพิ่มโอกาสในการโจมตีอย่างต่อเนื่อง ข้อมูลเกี่ยวกับโครงสร้างระบบและการตั้งค่า อาจช่วยให้ผู้โจมตีวิเคราะห์สภาพแวดล้อมของหน่วยงาน และใช้เป็นข้อมูลประกอบการโจมตีเพิ่มเติม เช่น การเคลื่อนย้ายภายในระบบ (Lateral Movement) หรือยกระดับสิทธิ์

ผลิตภัณฑ์ที่ได้รับผลกระทบ

ผลิตภัณฑ์ที่ได้รับผลกระทบ ได้แก่

- Vite v7.1.0 to v7.3.1
- Vite Vite v8.0.0 to v8.0.4

ผู้ใช้งานควรดำเนินการอัปเดตเป็นเวอร์ชันที่ได้รับการแก้ไขแล้ว ได้แก่

- Vite v7.3.2 or later
- Vite v8.0.5 or later

ระบบที่ควรตรวจสอบ

หน่วยงานที่มีการใช้งาน Vite ควรตรวจสอบระบบดังต่อไปนี้

1. ระบบเว็บไซต์หรือ Web Application ที่พัฒนาด้วย Vite และเปิดให้บริการผ่านอินเทอร์เน็ต
2. ระบบ Development หรือ Testing Environment ที่เปิดให้บุคคลภายนอกสามารถเข้าถึงได้
3. ระบบที่มีการจัดเก็บไฟล์ตั้งค่า ข้อมูลเชื่อมต่อบริการ หรือข้อมูลสำคัญภายในเครื่องที่ใช้งาน Vite

แนวทางป้องกันและแก้ไข

1. อัปเดต Vite เป็นเวอร์ชันล่าสุดที่ได้รับการแก้ไขแล้ว เพื่อป้องกันการใช้ประโยชน์จากช่องโหว่ดังกล่าว
2. หลีกเลี่ยงการเปิด Vite Development Server ผ่านอินเทอร์เน็ตโดยตรง หากไม่มีความจำเป็นควรจำกัดการเข้าถึงเฉพาะผู้เกี่ยวข้อง
3. ควรตรวจสอบ Log และระบบเฝ้าระวังความปลอดภัย เช่น Web Server Log, Firewall, WAF หรือ SIEM เพื่อค้นหาการเข้าถึงไฟล์ผิดปกติ
4. ควรตรวจสอบและเปลี่ยนข้อมูลยืนยันตัวตนที่เกี่ยวข้อง เช่น Password, API Key, Token หรือ Credentials หากพบว่าระบบเคยเปิดเผยต่ออินเทอร์เน็ต
5. ทำการแยกระบบ Development, Testing และ Production Environment พร้อมกำหนดสิทธิ์การเข้าถึงให้เหมาะสมตามหลัก Least Privilege

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้หน่วยงานที่ใช้งาน Vite Development Server ควรตรวจสอบระบบโดยเร็ว โดยเฉพาะระบบที่เปิดให้เข้าถึงจากอินเทอร์เน็ต และดำเนินการอัปเดตซอฟต์แวร์ รวมถึงตรวจสอบการเข้าถึงไฟล์สำคัญ เพื่อป้องกันการรั่วไหลของข้อมูลและลดความเสี่ยงจากการถูกโจมตีต่อเนื่องและสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th หรือ Scan QR Code

https://webboard-nsoc.ncsa.or.th

อ้างอิง

1. https://dg.th/7vg5lbzxr4
2. https://dg.th/wz3oadm1eb
3. https://dg.th/sx3kfjmoah