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

แจ้งเตือน การโจมตีแบบ Supply Chain Attack ผ่าน npm (Node Package Manager) ที่ใช้สำหรับการพัฒนาซอฟต์แวร์

วันที่แจ้งเตือน 24 กันยายน 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ThaiCERT สกมช. ได้เผยแพร่รายงานกรณีการโจมตีแบบ Supply Chain Attack โดยผู้ไม่หวังดีทำการโจมตีแบบ Social Engineering (Phishing) เพื่อเข้าถึงบัญชีของผู้ดูแลแพ็กเกจ npm* (Node Package Manager) และ ทำการฝังมัลแวร์และโค้ดอันตรายลงในแพ็กเกจดังกล่าว ทั้งนี้ พบว่าโค้ดอันตรายมีความสามารถในการแพร่กระจาย โดยมุ่งเป้าไปที่แพ็กเกจอื่น ๆ ของผู้ดูแลรายเดียวกัน และนำไปสู่การฝังโค้ดอันตรายเข้าไปยังแพ็กเกจที่ผู้พัฒนาซอฟต์แวร์นิยมนำมาใช้งาน เช่น debug และ chalk เป็นต้น

แพ็กเกจ npm version ที่ได้รับผลกระทบ		รายละเอียด	ผลกระทบ
• ansi-styles 6.2.2 • debug 4.4.2 • chalk 5.6.1 • supports-color 10.2.1 • strip-ansi 7.1.1 • ansi-regex 6.2.1 • wrap-ansi 9.0.1 • color-convert 3.1.1 • color-name 2.0.1 • is-arrayish 0.3.3	• slice-ansi 7.1.1 • color 5.0.1 • color-string 2.1.1 • simple-swizzle 0.2.3 • supports-hyperlinks 4.1.1 • has-ansi 6.0.1 • chalk-template 1.1.1 • backslash 0.2.1	โค้ดอันตรายจะถูกฝังลงในไฟล์ index.js ซึ่งจะทำหน้าที่ในการดักจับข้อมูลผ่านเบราว์เซอร์ โดยสามารถแทรกแซงการรับส่งข้อมูลเครือข่ายและ API ของแอปพลิเคชันได้ ซึ่งจะส่งผลกระทบเฉพาะผู้ใช้งานที่เข้าถึงแอปพลิเคชันที่ถูกโจมตีผ่านทางเว็บเท่านั้น รวมทั้งโค้ดอันตรายดังกล่าวอาจทำการตรวจสอบธุรกรรมที่เกี่ยวข้องกับคริปโต และเปลี่ยนแปลง wallet addresses ปลายทางไปยังกระเป๋าเงินที่ผู้ไม่หวังดีควบคุมอยู่ได้	• Applications และบริการที่อัปเดตโดยอัตโนมัติอาจนำโค้ดอันตรายเข้าสู่ applications และแพร่กระจายไปยัง applications อื่น ๆ ได้ • มัลแวร์อาจถูกติดตั้งภายใน Build Server และ Production ส่งผลให้ข้อมูลสำคัญรั่วไหลหรือถูกขโมย • ผู้ใช้งานปลายทาง โดยเฉพาะผู้ที่ใช้กระเป๋าเงินคริปโต (Cryptocurrency Wallet) อาจถูกดักจับหรือเปลี่ยนเส้นทางธุรกรรมไปยังกระเป๋าที่ผู้โจมตีได้

แนวทางการป้องกันและลดผลกระทบ:

- ตรวจสอบ (logs) ค้นหา lockfiles เช่น package-lock.json, pnpm-lock.yaml, yarn.lock เป็นต้น และใน Artifact Registry ว่ามีเวอร์ชันที่ตรงกับรายชื่อ แพ็กเกจ npm ที่ได้รับผลกระทบหรือไม่
- เปลี่ยนรหัสผ่าน และ Token ของระบบ CI/CD (Continuous Integration/Continuous Delivery) โดยทันทีหากพบการใช้งานแพ็กเกจที่ติดมัลแวร์ และทำการกักกัน และแยกระบบที่สงสัยออกจากระบบอื่น ๆ
- เฝ้าระวังและตรวจสอบการเชื่อมต่อไปยังโดเมน webhook[.]site ที่ผู้ไม่หวังดีใช้ในการแพร่กระจายมัลแวร์ หากไม่จำเป็นต้องใช้งานโดเมนดังกล่าวภายในระบบ ควรพิจารณาดำเนินการปิดกั้นการเข้าถึงเพื่อป้องกันความเสี่ยง

* npm ตัวจัดการแพ็กเกจ (package manager) และแหล่งรวมซอฟต์แวร์โอเพนซอร์ส (software registry) ที่ช่วยให้นักพัฒนาสามารถค้นหา ดาวน์โหลด จัดการ และติดตั้งไลบรารีหรือโมดูลต่าง ๆ มาใช้ในโปรเจกต์ JavaScript และ Node.js สำหรับการพัฒนาเว็บไซต์และแอปพลิเคชัน โดยองค์กรจำนวนมากมีการนำ npm มาใช้ในการบริหารจัดการการพัฒนาซอฟต์แวร์สำหรับใช้งานภายในองค์กร โดยนักพัฒนาสามารถแบ่งปันและใช้งานโค้ดที่คนอื่นสร้างไว้

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อผู้ประกอบธุรกิจในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 24 ก.ย. 2568
2) https://www.bleepingcomputer.com/news/security/hackers-hijack-npm-packages-with-2-billion-weekly-downloads-in-supply-chain-attack/
3) https://www.aikido.dev/blog/npm-debug-and-chalk-packages-compromised
4) https://www.paloaltonetworks.com/blog/cloud-security/npm-supply-chain-attack/