เอกสารแจ้งเตือนพบการโจมตีช่องโหว่บน JFrog Artifactory, ConnectWise ScreenConnect และ MikroTik RouterOS

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์กรณีพบการโจมตีช่องโหว่บน JFrog Artifactory, ConnectWise ScreenConnect และ MikroTik RouterOS นั้น

หน่วยงานความมั่นคงไซเบอร์และโครงสร้างพื้นฐานของสหรัฐฯ (CISA) ได้เพิ่มช่องโหว่ด้านความปลอดภัยใหม่ จำนวน 5 รายการลงในบัญชี Known Exploited Vulnerabilities (KEV) หลังพบรายงานการโจมตีจริงแล้ว โดยความเสี่ยงครอบคลุมตั้งแต่การข้ามการยืนยันตัวตน การยกระดับสิทธิ์ ไปจนถึงการลอบรันโปรแกรมอันตราย ซึ่งอาจส่งผลให้ผู้โจมตีสามารถเข้าควบคุมระบบได้โดยสมบูรณ์ ผู้ที่ได้รับผลกระทบคือองค์กรและหน่วยงานที่ใช้งานผลิตภัณฑ์ JFrog Artifactory, ConnectWise ScreenConnect และ MikroTik RouterOS จึงขอให้ผู้ดูแลระบบเร่งอัปเดตแพตช์ความปลอดภัยตามมาตรฐานของผลิตภัณฑ์ทันที[1]

<u>รายละเอียดช่องโหว่</u>

- CVE-2026-42016 (คะแนน CVSSv3.1: 8.1)[2] เป็นช่องโหว่จากการตรวจสอบสิทธิ์ที่ไม่ถูกต้อง (Incorrect Authorization) ใน JFrog Artifactory เกิดจากการตรวจสอบเพียงลายเซ็นหรือผู้ออกโทเค็น (Token Signature/Issuer) โดยไม่ได้ตรวจสอบขอบเขตสิทธิ์ของโทเค็น (Token Scope)
- CVE-2026-42018 (คะแนน CVSSv3.1: 7.5)[3] เป็นช่องโหว่จากการพิสูจน์ตัวตนที่ไม่เหมาะสม (Improper Authentication) ใน JFrog Artifactory ซึ่งอาจส่งคืน Anonymous-User Token ภายในให้กับผู้เรียกใช้ที่ไม่ได้รับการยืนยันตัวตน แม้จะมีการปิดใช้งาน Anonymous Access ไว้ก็ตาม
- CVE-2026-84869 (คะแนน CVSSv3.1: 9.9)[4] เป็นช่องโหว่จากการจัดการสิทธิ์และการอนุมัติที่ไม่เหมาะสม (Improper Privilege Management / Missing Authorization) ใน ConnectWise Screen Connect Client
- CVE-2026-67277 (คะแนน CVSSv3.1: 8.8)[5] เป็นช่องโหว่จากการขาดการพิสูจน์ตัวตนในฟังก์ชันสำคัญ (Missing Authentication for Critical Function) บนบริการ btest ของ MikroTik RouterOS
- CVE-2026-86060 (คะแนน CVSSv3.1: 9.2)[6] เป็นช่องโหว่จากการประมวลผลตัวแบ่งอาร์กิวเมนต์ในคำสั่งที่ไม่เหมาะสม (Improper Neutralization of Argument Delimiters in a Command) ใน MikroTik RouterOS

<u>ลักษณะการโจมตี</u>

- JFrog Artifactory: ผู้โจมตีใช้เทคนิค Exploit Chaining โดยเชื่อมโยงช่องโหว่ CVE-2026-42016 และ CVE-2026-42018 ร่วมกับ CVE-2026-82329 (CVSS 9.8) เพื่อข้ามการยืนยันตัวตน ยกระดับสิทธิ์เข้าควบคุมระบบในระดับผู้ดูแลระบบ (Administrator) จากนั้นจะสร้างบัญชีผู้ดูแลระบบแฝงฝัง ติดตั้งปลั๊กอิน Groovy ที่เป็นอันตรายเพื่อรันคำสั่ง และลง Backdoor ภาษา Rust เพื่อคงสิทธิ์การเข้าถึงระบบไว้ในระยะยาว
- ConnectWise ScreenConnect: ผู้โจมตีอาศัยช่องโหว่ฝั่ง Client ในการส่งไฟล์ VBScript ที่เป็นอันตราย และสั่งประมวลผลผ่าน Remote Session ที่ใช้งานอยู่ โดยไม่ต้องได้รับการยินยอมหรือยืนยันจากเครื่อง Host
- MikroTik RouterOS: ผู้โจมตีใช้เทคนิคการโจมตีที่เรียกว่า MikroTrick โดยเชื่อมโยงทั้งสองช่องโหว่เข้าด้วยกัน เพื่อดึงข้อมูลในหน่วยความจำ Kernel (Kernel Memory Disclosure), ก่อให้เกิดภาวะปฏิเสธการให้บริการ (DoS) ในบริการ btest รวมถึงแก้ไข Trusted Policy Mask เพื่อยกระดับสิทธิ์และเข้าควบคุมอุปกรณ์โดยไม่ต้องผ่านการยืนยันตัวตน

ผลกระทบ

- JFrog Artifactory: ถูกยึดสิทธิ์ผู้ดูแลระบบ (Admin Control), ถูกสร้างบัญชีแฝงฝัง (Persistent Admin), ถูกรันคำสั่งอันตรายผ่าน Groovy Plugin และถูกติดตั้ง Rust-based Backdoor เพื่อค้างอยู่ในระบบระยะยาว รวมถึงเสี่ยงต่อการรั่วไหลของข้อมูลสำคัญ

- ConnectWise ScreenConnect: ผู้โจมตีสามารถส่งไฟล์และสั่งประมวลผล VBScript Payload บนเครื่องปลายทาง (Host Client) ด้วยสิทธิ์ระดับสูง

- MikroTik RouterOS: ข้อมูลในหน่วยความจำ Kernel รั่วไหล, ระบบหยุดทำงานจากภาวะปฏิเสธการให้บริการ (DoS) และถูกเปลี่ยน Policy Mask เพื่อยกระดับสิทธิ์เข้าควบคุมอุปกรณ์ทั้งหมด

ผลิตภัณฑ์ที่ได้รับผลกระทบ

- JFrog Artifactory (รุ่น Self-hosted)
- ConnectWise ScreenConnect (กระทบเฉพาะฝั่ง Client ไม่ส่งผลกระทบต่อฝั่ง Server)
- MikroTik RouterOS

แนวทางการแก้ไขและป้องกัน

- JFrog Artifactory ดำเนินการอัปเดตแพตช์ความปลอดภัยล่าสุดจากผู้พัฒนา เพื่ออุดช่องโหว่การยืนยันตัวตนและการตรวจสอบสิทธิ์

- ConnectWise ScreenConnect อัปเดต ScreenConnect ให้เป็นเวอร์ชัน 26.6.5 หรือใหม่กว่าโดยเร็ว

- MikroTik RouterOS อัปเดตระบบปฏิบัติการ RouterOS เป็นเวอร์ชันล่าสุดเพื่อแก้ไขช่องโหว่ความปลอดภัยในบริการ btest และการจัดการ Policy Mask

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้ผู้ใช้งานและผู้ดูแลระบบตรวจสอบเวอร์ชันของผลิตภัณฑ์ รวมทั้งดำเนินการอัปเดตซอฟต์แวร์หรือใช้มาตรการลดความเสี่ยงตามคำแนะนำโดยเร็ว เพื่อป้องกันความเสี่ยงที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ นอกจากนี้ควรเฝ้าระวังกิจกรรมที่ผิดปกติหรือพฤติกรรมที่อาจบ่งชี้ถึงการถูกโจมตีหรือการเข้าถึงระบบโดยไม่ได้รับอนุญาต เพื่อรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและการให้บริการที่สำคัญอย่างต่อเนื่อง ทั้งนี้ สามารถติดตามข่าวสารและคำแนะนำด้านภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

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

อ้างอิง

1. https://dg.th/tb1mg8o7vl
2. https://dg.th/0j2d4x6lob
3. https://dg.th/sopnb5cm0a
4. https://dg.th/dyn8ozsurl
5. https://dg.th/wfachq3yt8
6. https://dg.th/l1ks9r4tch