วันที่ 20 กุมภาพันธ์ 2569

Notepad++ ออกแพตช์แก้ไขช่องโหว่ระบบอัปเดตที่ถูกยึดไปใช้แพร่กระจายมัลแวร์

Notepad++ โปรแกรมแก้ไขข้อความยอดนิยม ออกอัปเดตความปลอดภัยเวอร์ชัน 8.9.2 เพื่อแก้ไขช่องโหว่ร้ายแรง หลังถูกกลุ่มภัยคุกคามขั้นสูง (APT) จากจีนเข้าแทรกแซงระบบอัปเดตเพื่อส่งมัลแวร์ไปยังเป้าหมายเฉพาะกลุ่ม ผู้ดูแลโครงการ Notepad++ ระบุว่าการอัปเดตครั้งนี้ใช้แนวคิด “Double Lock” เพื่อยกระดับความปลอดภัยให้แข็งแกร่งจนยากต่อการโจมตี โดยมีกลไกหลักดังนี้:

1. ตรวจสอบตัวติดตั้งที่มีลายเซ็นดิจิทัลของไฟล์ที่ดาวน์โหลดจาก GitHub (เริ่มใช้ตั้งแต่เวอร์ชัน 8.8.9)
2. เพิ่มการตรวจสอบลายเซ็นดิจิทัลของไฟล์ XML ที่ส่งกลับมาจากเซิร์ฟเวอร์หลัก notepad-plus-plus[.]org

เสริมเกราะป้องกันให้ตัวอัปเดตอัตโนมัติ

นอกจากกลไกล็อกสองชั้นแล้ว ยังมีการปรับปรุงส่วนประกอบ WinGUp เพื่อลดความเสี่ยงจากการถูกโจมตีทางเทคนิค ดังนี้:

- ป้องกันมัลแวร์แฝง: ลบไฟล์ libcurl.dll ทิ้ง เพื่อปิดช่องว่างไม่ให้แฮกเกอร์ใช้เทคนิค *DLL side-loading*
- ปิดช่องโหว่ SSL: ยกเลิกตัวเลือกที่ไม่ปลอดภัยใน cURL ได้แก่ CURLSSLOPT_ALLOW_BEAST และ CURLSSLOPT_NO_REVOKE
- คัดกรองปลั๊กอิน: จำกัดให้ระบบจัดการปลั๊กอินรันได้เฉพาะโปรแกรมที่ลงลายเซ็นด้วยใบรับรองเดียวกับ WinGUp เท่านั้น

แก้ไขช่องโหว่รันรหัสอันตราย (RCE)

การอัปเดตนี้ยังแก้ช่องโหว่ระดับ High Risk (รหัส CVE-2026-25926, คะแนน CVSS 7.3) ซึ่งอาจทำให้แฮกเกอร์รันโค้ดอันตรายผ่านแอปพลิเคชันได้ ช่องโหว่ประเภท Unsafe Search Path (CWE-426) นี้เกิดขึ้นเมื่อโปรแกรมเรียกใช้ Windows Explorer โดยไม่ระบุพาธไฟล์แบบเต็ม ทำให้แฮกเกอร์อาจหลอกให้ระบบไปรันไฟล์ explorer.exe ที่เป็นมัลแวร์เพื่อยึดสิทธิ์การทำงานของแอปพลิเคชันได้

เบื้องหลังการโจมตี กลุ่ม Lotus Panda และมัลแวร์ Chrysalis

เหตุการณ์นี้สืบเนื่องมาจากเมื่อไม่กี่สัปดาห์ก่อน Notepad++ ตรวจพบการบุกรุกในระดับผู้ให้บริการโฮสติ้ง ทำให้แฮกเกอร์ยึดทราฟฟิกการอัปเดตได้ตั้งแต่เดือนมิถุนายน 2025 และเปลี่ยนเส้นทางคำขออัปเดตของผู้ใช้บางรายไปยังเซิร์ฟเวอร์อันตรายเพื่อส่งไฟล์ปลอม จากการวิเคราะห์พบว่าแฮกเกอร์ใช้ช่องทางนี้ส่งแบ็กดอร์ตัวใหม่ชื่อ "Chrysalis" (รหัส CVE-2025-15556) โดยเชื่อมโยงกับกลุ่มแฮกเกอร์จีนชื่อ Lotus Panda

เป้าหมายการโจมตี ครอบคลุมหลายประเทศ เช่น เวียดนาม, ฟิลิปปินส์, สหรัฐฯ, ออสเตรเลีย รวมถึงในยุโรปและอเมริกาใต้ มุ่งเน้นกลุ่มอุตสาหกรรมการเงินและภาครัฐ, พลังงานและการผลิต, โฮสติ้งคลาวด์ และผู้พัฒนาซอฟต์แวร์

คำแนะนำสำหรับผู้ใช้: ให้รีบอัปเดต Notepad++ เป็นเวอร์ชัน 8.9.2 ทันที และควรดาวน์โหลดจากเว็บไซต์ทางการเท่านั้นเพื่อความปลอดภัย

ข้อมูลอ้างอิง

Feb 18, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/02/notepad-fixes-hijacked-update-mechanism.html