วันที่ 18 เมษายน 2568

เตือนภัย ช่องโหว่ Remote Code Execution บน Erlang/OTP

Executive Summary

นักวิจัยจากมหาวิทยาลัย Ruhr เมืองโบชุม ค้นพบช่องโหว่ร้ายแรงที่เรียกว่า CVE-2025-32433 ใน Daemon SSH ของ Erlang/OTP ซึ่งทำให้สามารถเรียกใช้โค้ดจากระยะไกลได้โดยไม่ผ่านการตรวจสอบสิทธิ์ (RCE) และได้รับการกำหนดให้มีระดับความรุนแรงสูงสุดที่ 10.0 ช่องโหว่นี้เกิดจากการจัดการข้อความโปรโตคอลก่อนการตรวจสอบสิทธิ์ที่ไม่เหมาะสมภายใน Daemon SSH ทำให้ผู้โจมตีสามารถเรียกใช้คำสั่งตามได้โดยไม่ต้องผ่านการตรวจสอบสิทธิ์ก่อน อุปกรณ์ทั้งหมดที่ใช้ Daemon SSH ของ Erlang/OTP มีความเสี่ยงและควรอัปเดตเป็นเวอร์ชั่นที่ได้รับการแก้ไขช่องโหว่แล้ว

CVE-2025-32433 (Erlang/OTP SSH RCE) เป็นช่องโหว่ความปลอดภัยร้ายแรงระดับ วิกฤต (Critical) ในระบบ SSH Server ของ Erlang/OTP ที่ช่วยให้ผู้โจมตีสามารถรันโค้ดจากระยะไกลได้โดยไม่ต้องยืนยันตัวตน (Unauthenticated Remote Code Execution)

Affected Versions

Erlang/OTP ที่ต่ำกว่าเวอร์ชั่น

- 25.3.2.20
- 26.2.5.11
- 27.3.3

คำแนะนำ (Recommendation)

- ดำเนินการปิดใช้งาน SSH Server ของ Erlang หากไม่จำเป็น
- อัปเดต Erlang/OTP ไปยังเวอร์ชั่นที่ได้รับการแก้ไขแล้ว
- การจำกัดการเข้าถึงไฟร์วอลล์ผ่านพอร์ต SSH

ข้อมูลอ้างอิง

- https://www.bleepingcomputer.com/news/security/critical-erlang-otp-ssh-pre-auth-rce-is-surprisingly-easy-to-exploit-patch-now/