ประจำวันจันทร์ที่ 6 มิถุนายน 2565

Atlassian ออก Patch สำหรับ Zero-Day Flaw Exploited in the Wild

เมื่อวันศุกร์ที่ผ่านมา Atlassian ได้เปิดตัวแพตช์เพื่อแก้ไขช่องโหว่ที่สำคัญ ซึ่งส่งผลต่อผลิตภัณฑ์ Confluence Server และ Data Center ที่อยู่ภายใต้การใช้ประโยชน์จากผู้โจมตีในการเรียกใช้โค้ดจากระยะไกล หมายเลขช่องโหว่ CVE-2022-26134 คล้ายกับหมายเลขช่องโหว่ CVE-2021-26084 ซึ่งเป็นช่องโหว่อีกหนึ่งที่บริษัทซอฟต์แวร์ของออสเตรเลียได้เคยแก้ไขในเดือนสิงหาคม 2564 ทั้งสองช่องโหว่เกี่ยวกับการ injection ของ Object-Graph Navigation Language (OGNL) ที่สามารถใช้ประโยชน์จากการเรียกใช้โค้ดโดยอำเภอใจบนเซิร์ฟเวอร์ Confluence หรือ Data Center instance

ช่องโหว่ที่ค้นพบใหม่ส่งผลกระทบต่อ Confluence Server และ Data Center ทุกรุ่นที่รองรับ โดยที่เวอร์ชันหลัง 1.3.0 ทุกเวอร์ชั่นจะได้รับผลกระทบด้วย ซึ่งเวอร์ชันที่ได้รับการแก้ไขแล้วมีต่อไปนี้

- 7.4.17
- 7.13.7
- 7.14.3
- 7.15.2
- 7.16.4
- 7.17.4
- 7.18.1

สำนักงานความมั่นคงปลอดภัยทางไซเบอร์และโครงสร้างพื้นฐานของสหรัฐอเมริกา (CISA) ของสหรัฐอเมริกา ได้เพิ่มช่องโหว่ Zero-Day ในแคตตาล็อกช่องโหว่ แล้วยังเรียกร้องให้หน่วยงานของรัฐบาลกลางปิดกั้นการรับส่งข้อมูลทางอินเทอร์เน็ตทั้งหมดไปจากผลิตภัณฑ์ที่ได้รับผลกระทบทันที และใช้การแพตช์หรือลบ อินสแตนซ์ภายในวันที่ 6 มิถุนายน 2022, 17.00 น. ET

ที่มาของข่าว : https://thehackernews.com/2022/06/atlassian-releases-patch-for-confluence.html