ประจำวันจันทร์ที่ 26 กันยายน 2565

Sophos ออกแพตช์แก้ไขช่องโหว่ RCE Zero-Day ในไฟร์วอลล์

บริษัทซอฟต์แวร์รักษาความปลอดภัย Sophos ได้ออกแพตช์อัปเดตไฟร์วอลล์ของบริษัท หลังจากที่พบว่าผู้โจมตีใช้ช่องโหว่ Zero-Day อันใหม่นี้เพื่อโจมตีเครือข่ายของลูกค้า ที่หมายเลขช่องโหว่ CVE-2022-3236 (คะแนน CVSS: 9.8) ส่งผลกระทบต่อ Sophos Firewall v19.0 MR1 (19.0.1) และเวอร์ชั่นที่เก่ากว่า ซึ่งช่องโหว่ดังกล่าวเป็นการแทรกโค้ดในพอร์ทัลผู้ใช้งาน และส่วนประกอบ Webadmin ที่อาจส่งผลให้เกิดโค้ดจากระยะไกลได้

บริษัทกล่าวว่าช่องโหว่นี้ถูกกำหนดเป้าหมายไปยังกลุ่มองค์กรเฉพาะ โดยเฉพาะในภูมิภาคเอเชียใต้ เพื่อเป็นการแก้ปัญหาชั่วคราว Sophos ขอแนะนำให้ทำตามขั้นตอนต่างๆ เพื่อให้ User Portal และ Webadmin จะไม่ถูกเปิดเผยต่อ WAN หรือผู้ใช้งานสามารถอัปเดตเป็นเวอร์ชันล่าสุดที่รองรับ

- v19.5 GA
- v19.0 MR2 (19.0.2)
- v19.0 GA, MR1 และ MR1-1
- v18.5 MR5 (18.5.5)
- v18.5 GA, MR1, MR1-1, MR2, MR3 และ MR4
- v18.0 MR3, MR4, MR5 และ MR6
- v17.5 MR12, MR13, MR14, MR15, MR16 และ MR17
- v17.0 MR10

ผู้ใช้ที่ใช้งาน Sophos Firewall เวอร์ชันเก่าจะต้องอัปเกรดเพื่อรับการป้องกันล่าสุดและการแก้ไขที่เกี่ยวข้อง

ครั้งนี้นับเป็นครั้งที่สองที่ช่องโหว่ของ Sophos Firewall ถูกโจมตีภายในหนึ่งปี เมื่อต้นเดือนมีนาคมนี้ ซึ่งช่องโหว่อีกรายการ (CVE-2022-1040) ถูกใช้กำหนดเป้าหมายไปที่องค์กรในภูมิภาคเอเชียใต้ จากนั้นในเดือนมิถุนายน บริษัทรักษาความปลอดภัยทางไซเบอร์ Volexity ได้เปิดเผยรายละเอียดเพิ่มเติมเกี่ยวกับแคมเปญการโจมตี โดยเป็นการโจมตีของภัยคุกคามขั้นสูงของจีน (APT) ที่รู้จักกันในชื่อ DriftingCloud

ที่มาของข่าว : https://thehackernews.com/2022/09/hackers-actively-exploiting-new-sophos.html