ประจำวันศุกร์ที่ 24 มิถุนายน 2565

ช่องโหว่ PHP ระดับวิกฤติที่ทำให้อุปกรณ์ QNAP NAS ถูกโจมตีจากระยะไกล

QNAP ผู้ผลิตอุปกรณ์ Network-attached Storage (NAS) ของไต้หวัน กล่าวว่ากำลังดำเนินขั้นตอนการแก้ไขช่องโหว่ PHP ที่สำคัญ ซึ่งอาจถูกนำไปใช้ในทางที่ผิดเพื่อให้เกิดการเรียกใช้โค้ดจากระยะไกลได้ ที่ส่งผลกระทบต่อ PHP เวอร์ชัน 7.1.x ต่ำกว่า 7.1.33, 7.2.x ต่ำกว่า 7.2.24 และ 7.3.x ต่ำกว่า 7.3.11 ด้วยการกำหนดค่า nginx ที่ไม่ถูกต้อง หากถูกโจมตี ช่องโหว่ดังกล่าวจะทำให้ผู้โจมตีสามารถเรียกใช้โค้ดจากระยะไกลได้

ช่องโหว่หมายเลข CVE-2019-11043 ได้รับการให้คะแนนที่ 9.8 จาก 10 ความรุนแรงในระบบการให้คะแนนช่องโหว่ CVSS ดังกล่าว ที่ Nginx และ php-fpm จะต้องทำงานในอุปกรณ์ที่ใช้ระบบปฏิบัติการ QNAP เวอร์ชันต่อไปนี้

- QTS 5.0.x and later
- QTS 4.5.x and later
- QuTS hero h5.0.x and later
- QuTS hero h4.5.x and later
- QuTScloud c5.0.x and later

เนื่องจาก QTS, QuTS hero ของ QuTS หรือ QuTScloud ไม่ได้ติดตั้ง nginx ตามค่าเริ่มต้น QNAP NAS จะไม่ได้รับผลกระทบจากช่องโหว่นี้จากการตั้งค่าเริ่มต้น บริษัทกล่าวได้แก้ไขปัญหาในระบบปฏิบัติการเวอร์ชัน QTS 5.0.1.2034 build 20220515 แล้ว QuTS hero QuTS h 5.0.0.2069 บิลด์ 20220614

QNAP เปิดเผยว่าได้ตรวจสอบอย่างละเอียดถึงการโจมตี DeadBolt ransomware ที่กำหนดเป้าหมายไปที่อุปกรณ์ QNAP NAS ที่ใช้ QTS 4.x เวอร์ชันเก่าและแนะนำให้ลูกค้าอัปเกรดระบบปฏิบัติการ QTS และ QuTS hero เวอร์ชันใหม่ล่าสุดแล้ว ยังแนะนำว่าอุปกรณ์ต่างๆ ไม่ควรถูกเปิดเผยต่ออินเทอร์เน็ต

ที่มาของข่าว : https://thehackernews.com/2022/06/critical-php-vulnerability-exposes-qnap.html