ประจำวันศุกร์ที่ 1 กรกฎาคม 2565

# ช่องโหว่ใหม่ของ UnRAR อาจทำให้ผู้โจมตีสามารถเข้าถึง Zimbra Webmail Servers ได้

ช่องโหว่ด้านความปลอดภัยใหม่ได้รับการเปิดเผยในยูทิลิตี UnRAR ของ RARlab ซึ่งหากถูกโจมตีสำเร็จ อาจอนุญาตให้ผู้โจมตีจากระยะไกลรันโค้ดตามอำเภอใจบนระบบ ซึ่งช่องโหว่หมายเลข CVE-2022-30333 เกี่ยวข้องกับช่องโหว่การข้ามเส้นทางใน UnRAR เวอร์ชัน Unix ที่สามารถทริกเกอร์ได้เมื่อแยกไฟล์เก็บถาวร RAR ที่ออกแบบมาเพื่อประสงค์ร้าย

เมื่อวันที่ 4 พฤษภาคม 2022 RarLab ได้แก้ไขช่องโหว่ดังกล่าวโดยเป็นส่วนหนึ่งของเวอร์ชัน 6.12 ที่เผยแพร่เมื่อวันที่ 6 พฤษภาคม โดยซอฟต์แวร์เวอร์ชันอื่นๆ รวมถึงเวอร์ชันสำหรับระบบปฏิบัติการ Windows และ Android จะไม่ได้รับผลกระทบ

นักวิจัยของ SonarSource Simon Scannell กล่าวว่าผู้โจมตีสามารถสร้างไฟล์นอกไดเร็กทอรีโดยการแยกเป้าหมายจะสามารถใช้ประโยชน์ในการดำเนินการคำสั่งตามอำเภอใจบนระบบ ซึ่งรวมถึงชุดการทำงานร่วมกันของ Zimbra ซึ่งช่องโหว่ดังกล่าวอาจนำไปสู่การเรียกใช้โค้ดจากระยะไกลที่ตรวจสอบสิทธิ์ล่วงหน้าบนอินสแตนซ์ที่มีช่องโหว่ ทำให้ผู้โจมตีสามารถเข้าถึงเซิร์ฟเวอร์อีเมลได้อย่างสมบูรณ์ หรือแม้แต่ละเมิดเพื่อเข้าถึงหรือเขียนทับทรัพยากรภายในอื่นๆ ภายในเครือข่ายขององค์กร

ช่องโหว่เกี่ยวข้องกับการ โจมตี ลิงก์สัญลักษณ์ซึ่งไฟล์เก็บถาวร RAR ถูกสร้างขึ้นเพื่อให้มี symlink ที่ผสมผสานระหว่างเครื่องหมายทับและแบ็กสแลช (เช่น "..\..\..\tmp/ เชลล์") เพื่อข้ามการตรวจสอบปัจจุบันและแยกออกนอกไดเร็กทอรี ซึ่งฟังก์ชันที่ออกแบบมาเพื่อแปลงแบ็กสแลช ('\') เป็นฟอร์เวิร์ดสแลช ('/') เพื่อให้สามารถแยกไฟล์เก็บถาวร RAR ที่สร้างบน Windows บนระบบ Unix ได้อย่างมีประสิทธิภาพแก้ไข symlink ดังกล่าว เป็น "../../../tmp/shell ด้วยการใช้ประโยชน์จากพฤติกรรมนี้ ผู้โจมตีสามารถเขียนไฟล์ใดก็ได้บนระบบไฟล์เป้าหมายโดยอำเภอใจ ซึ่งรวมถึงการสร้างเชลล์ JSP ในไดเร็กทอรีเว็บของ Zimbra และดำเนินการคำสั่งที่เป็นอันตราย

ที่มาของข่าว : https://thehackernews.com/2022/06/new-unrar-vulnerability-could-let.html