วันที่ 19 กุมภาพันธ์ 2569

พบช่องโหว่ Zero-Day ร้ายแรงใน Dell RecoverPoint for VMs (CVE-2026-22769) ถูกโจมตีต่อเนื่องตั้งแต่กลางปี 2024

รายงานล่าสุดจาก Google Mandiant และ Google Threat Intelligence Group (GTIG) เปิดเผยความเคลื่อนไหวที่น่ากังวลของกลุ่มภัยคุกคามสัญชาติจีนชื่อ UNC6201 ที่เริ่มปฏิบัติการมาตั้งแต่กลางปี 2024 โดยมุ่งเป้าเจาะระบบสำรองข้อมูลชื่อดังอย่าง Dell RecoverPoint for Virtual Machines

รายละเอียดเทคนิคของช่องโหว่

ช่องโหว่ดังกล่าวมีรหัส CVE-2026-22769 ซึ่งได้รับคะแนนความรุนแรงเต็ม 10.0 (CVSS score) สาเหตุเกิดจากการมี Hard-coded credentials หรือการตั้งชื่อผู้ใช้และรหัสผ่านตายตัวไว้ในระบบ (Admin ของ Apache Tomcat Manager) ซึ่งส่งผลกระทบต่อเวอร์ชันที่ต่ำกว่า 6.0.3.1 HF1

Dell ระบุว่า ช่องโหว่นี้ถือว่าร้ายแรงมาก แฮกเกอร์ที่รู้รหัสลับนี้สามารถบุกรุกเข้าสู่ระบบปฏิบัติการได้โดยไม่ต้องยืนยันตัวตน และสามารถฝังตัวอยู่ในระบบในระดับ "Root" (สิทธิ์สูงสุด) ได้อย่างถาวร

ผลิตภัณฑ์ที่ได้รับผลกระทบและแนวทางแก้ไข

ปัญหาความปลอดภัยนี้ส่งผลกระทบโดยตรงต่อผลิตภัณฑ์ RecoverPoint for Virtual Machines ในเวอร์ชันต่างๆ ดังนี้:

- **เวอร์ชัน 5.3 SP4 P1:** แนะนำให้เปลี่ยนจากเวอร์ชัน 5.3 SP4 P1 ไปเป็นเวอร์ชัน 6.0 SP3 ก่อน จากนั้นจึงดำเนินการอัปเกรดต่อไปยังเวอร์ชัน 6.0.3.1 HF1
- **เวอร์ชัน 6.0, 6.0 SP1, 6.0 SP1 P1, 6.0 SP1 P2, 6.0 SP2, 6.0 SP2 P1, 6.0 SP3 และ 6.0 SP3 P1:** แนะนำให้ดำเนินการอัปเกรดเป็นเวอร์ชัน 6.0.3.1 HF1 ได้ทันที
- **เวอร์ชัน 5.3 SP4, 5.3 SP3, 5.3 SP2 และเวอร์ชันก่อนหน้า:** แนะนำให้อัปเกรดเป็นเวอร์ชัน 5.3 SP4 P1 หรือเวอร์ชันในตระกูล 6.x จากนั้นให้ดำเนินการแก้ไขเพิ่มเติมตามรายละเอียดที่ระบุในคำแนะนำ

นอกจากนี้ ทาง Dell ได้เน้นย้ำคำแนะนำว่า ควรติดตั้ง RecoverPoint for Virtual Machines ไว้ภายในเครือข่ายภายในที่เชื่อถือได้เท่านั้น โดยต้องมีการควบคุมสิทธิ์การเข้าถึงอย่างเข้มงวด มีการป้องกันด้วยไฟร์วอลล์ และมีการแบ่งส่วนเครือข่ายที่เหมาะสม เนื่องจากผลิตภัณฑ์นี้ไม่ได้ถูกออกแบบมาเพื่อใช้งานบนเครือข่ายสาธารณะหรือเครือข่ายที่ไม่น่าเชื่อถือ

อาวุธและเทคนิคเหนือชั้นของ UNC6201

Google ระบุว่าบัญชี hard-coded เป็นบัญชี “admin” ของ Apache Tomcat Manager ซึ่งผู้โจมตีใช้ในการอัปโหลด web shell ชื่อ SLAYSTYLE ผ่าน endpoint "/manager/text/deploy" ก่อนรันคำสั่งในระดับ root เพื่อวาง backdoor BRICKSTORM และเวอร์ชันใหม่ชื่อว่า GRIMBOLT

Google เสริมว่า GRIMBOLT เป็น backdoor ที่เขียนด้วย C# และคอมไพล์แบบ AOT (Ahead-of-Time) ทำให้วิเคราะห์ย้อนกลับได้ยากขึ้น โดยเป้าหมายส่วนใหญ่เป็นองค์กรในอเมริกาเหนือ และ GRIMBOLT มีการพัฒนาเพื่อหลบการตรวจจับและลดร่องรอยนิติวิทยาศาสตร์ โดย “กลมกลืนกับไฟล์ระบบได้แนบเนียนกว่าเดิม”

ความเชื่อมโยงกับกลุ่มจารกรรมไซเบอร์อื่นๆ

มีการประเมินว่า UNC6201 อาจมีความเชื่อมโยงบางส่วนกับกลุ่มจารกรรมไซเบอร์ของจีนชื่อ UNC5221 ซึ่งเคยใช้ช่องโหว่ virtualization และ Ivanti zero-day ในการแพร่กระจาย web shells และมัลแวร์อย่าง BEEFLUSH, BRICKSTORM และ ZIPLINE แต่ทั้งสองกลุ่มยังคงถูกจัดว่าเป็นกลุ่มแยกกัน

นอกจากนี้ CrowdStrike ยังเชื่อมโยงการใช้ BRICKSTORM กับกลุ่มจีนอีกกลุ่มชื่อ Warp Panda ซึ่งโจมตีหน่วยงานในสหรัฐฯ

เทคนิค "Ghost NICs" และการพรางตัวบน Appliance

จุดที่น่าสนใจของเหตุการณ์ล่าสุดคือ UNC6201 ใช้ Virtual NIC ชั่วคราว (“Ghost NICs”) เพื่อโจมตีจาก VM ที่ถูกบุกรุกไปยังระบบภายในหรือ SaaS แล้วลบ NIC เหล่านั้นเพื่อกลบหลักฐาน

Google ระบุว่าเหมือนกับแคมเปญ BRICKSTORM ก่อนหน้า UNC6201 ยังคงมุ่งเป้าระบบ appliance ที่มักไม่มี EDR ทำให้สามารถซ่อนตัวได้นานมาก

การเข้าถึงระยะแรกและการควบคุมผ่าน iptables

ยังไม่ชัดเจนว่าผู้โจมตีเจาะระบบครั้งแรกได้อย่างไร แต่มีพฤติกรรมคล้าย UNC5221 ที่มักใช้ช่องโหว่ edge appliance เพื่อเข้าสู่เครือข่ายเป้าหมาย การวิเคราะห์ VMware vCenter ที่ถูกเจาะพบการรันคำสั่ง iptables เพื่อ:

- ดัก traffic บนพอร์ต 443 ที่มี HEX pattern เฉพาะ
- หาก IP อยู่ในรายการ whitelist ให้เชื่อมต่อพอร์ต 10443 จะอนุญาตให้เชื่อมต่อได้
- และ redirect การสื่อสารจากพอร์ต 443 ไป 10443 เป็นเวลา 300 วินาที หากอยู่ใน whitelist

การยกระดับเครื่องมือจาก BRICKSTORM สู่ GRIMBOLT

นอกจากนี้ ยังพบว่าผู้โจมตีถูกพบว่าเปลี่ยน BRICKSTORM เป็น GRIMBOLT ตั้งแต่กันยายน 2025 ทั้งสองตัวใช้เซิร์ฟเวอร์ควบคุม (C2) เดียวกันแต่ยังไม่ชัดว่าเปลี่ยนเพราะต้องการยกระดับการหลบตรวจจับ หรือเพราะมีข้อมูล BRICKSTORM ถูกเปิดเผยสู่สาธารณะ

Carmakal จาก Google ทิ้งท้ายว่า “ผู้โจมตีระดับรัฐชาติยังคงมุ่งเป้าระบบที่ไม่รองรับ EDR ทำให้องค์กรไม่รู้ว่าถูกเจาะ และเพิ่มเวลาการฝังตัวอย่างมาก”

การขยายวงโจมตีสู่ระบบโครงสร้างพื้นฐาน (OT)

ในอีกด้านหนึ่ง บริษัท Dragos เตือนถึงการโจมตีของกลุ่มจีน เช่น Volt Typhoon (Voltzite) ที่เจาะอุปกรณ์ Sierra Wireless Airlink ในภาคไฟฟ้าและน้ำมัน ก่อนขยายไปยัง engineering workstation เพื่อดึง config และ alarm data เหตุการณ์เกิดขึ้นในเดือนกรกฎาคม 2025 โดยเริ่มจากการใช้ช่องโหว่ edge device ผ่านกลุ่ม Sylvanite

Dragos ระบุว่า Voltzite ไม่เพียงขโมยข้อมูล แต่ยังเริ่มทดลอง “ควบคุมหรือหยุดกระบวนการทำงานจริง” ซึ่งเป็นสัญญาณอันตรายเพราะเป็นการลบกำแพงสุดท้ายระหว่างการเข้าถึงกับผลกระทบทางกายภาพ

ข้อมูลอ้างอิง

Feb 18, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/02/dell-recoverpoint-for-vms-zero-day-cve.html