วันที่ 2 ตุลาคม 2568

ด่วน : แฮกเกอร์ที่เชื่อมโยงกับจีนใช้ประโยชน์จากช่องโหว่ Zero-Day ใหม่ของ VMware

นักวิจัยด้านความปลอดภัยได้ออกมาเปิดเผยว่า ช่องโหว่ความปลอดภัยที่เพิ่งได้รับการแพตช์แล้วซึ่งกระทบกับ Broadcom VMware Tools และ VMware Aria Operations ถูกนำมาใช้โจมตีในสภาพแวดล้อมจริงตั้งแต่กลางเดือนตุลาคม 2024 โดยกลุ่มปฏิบัติการที่เชื่อมโยงกับจีนที่ชื่อ UNC5174 ตามรายงานของ NVISO Labs

แม้ Broadcom จะไม่ได้กล่าวถึงการถูกนำไปใช้โจมตีในโลกจริง แต่รายงานนี้ยืนยันว่าช่องโหว่นี้ไม่ได้เป็นแค่ภัยคุกคามทางทฤษฎีอีกต่อไป และได้ถูกเชื่อมโยงกับกลุ่มแฮกเกอร์ที่มีประวัติใช้ประโยชน์จากช่องโหว่ต่างๆ รวมถึงที่กระทบ Ivanti และ SAP NetWeaver เพื่อเข้าถึงระบบเป้าหมาย

เวอร์ชันที่ได้รับผลกระทบมีดังนี้:

- VMware Cloud Foundation 4.x และ 5.x
- VMware Cloud Foundation 9.x.x.x และ 13.x.x.x (Windows, Linux)
- VMware vSphere Foundation 9.x.x.x และ 13.x.x.x (Windows, Linux)
- VMware Aria Operations 8.x
- VMware Tools 11.x.x, 12.x.x และ 13.x.x (Windows, Linux)
- VMware Telco Cloud Platform 4.x และ 5.x
- VMware Telco Cloud Infrastructure 2.x และ 3.x

นักวิจัยจาก NVISO Labs ได้เปิดเผยข้อมูลที่น่าตกใจว่าช่องโหว่ความปลอดภัยที่เพิ่งได้รับการแพตช์ ซึ่งส่งผลกระทบต่อ Broadcom VMware Tools และ VMware Aria Operations ถูกนำไปใช้โจมตีในสภาพแวดล้อมจริงแล้วตั้งแต่กลางเดือนตุลาคม 2024 โดยกลุ่มปฏิบัติการที่เชื่อมโยงกับจีนที่ชื่อ UNC5174

แม้ Broadcom จะไม่ได้กล่าวถึงการโจมตีในโลกจริง แต่รายงานนี้ได้เชื่อมโยงช่องโหว่ดังกล่าวกับกลุ่มแฮกเกอร์ที่ทาง Mandiant (Google) ติดตามในชื่อ UNC5174 (หรือที่รู้จักในชื่อ Uteus หรือ Uetus) ซึ่งมีประวัติการใช้ประโยชน์จากช่องโหว่ต่างๆ รวมถึงที่กระทบ Ivanti และ SAP NetWeaver เพื่อเข้าถึงระบบเป้าหมาย

ช่องโหว่ CVE-2025-41244: การยกระดับสิทธิ์ภายในเครื่อง

ช่องโหว่ดังกล่าวคือ CVE-2025-41244 ซึ่งเป็นข้อบกพร่องแบบ local privilege escalation (ยกระดับสิทธิ์ภายในเครื่อง)

คำเตือนจาก VMware: VMware ได้ระบุไว้ในคำแนะนำเมื่อวันจันทร์ว่า “ผู้โจมตีที่เป็นผู้ใช้ภายในเครื่อง (local) ซึ่งไม่มีสิทธิ์ระดับแอดมิน แต่มีสิทธิ์เข้าใช้งาน VM ที่ติดตั้ง VMware Tools และถูกจัดการโดย Aria Operations ที่เปิดใช้งาน SDMP อาจสามารถใช้ช่องโหว่นี้ยกระดับสิทธิ์เป็น root บน VM เดียวกันได้” การเป็นช่องโหว่แบบ local นี้หมายความว่า ผู้โจมตีจำเป็นต้องมีช่องทางเข้าถึงเครื่องที่ถูกโจมตีก่อนแล้วด้วยวิธีอื่น

นักวิจัย Maxime Thiebaut จาก NVISO ได้รับเครดิตในการค้นพบและรายงานช่องโหว่นี้เมื่อวันที่ 19 พฤษภาคม 2025 ในขณะปฏิบัติภารกิจตอบสนองเหตุการณ์

กลไกทางเทคนิค: การหลอกล่อฟังก์ชันด้วย Regex

NVISO ระบุว่าช่องโหว่นี้มีต้นเหตุมาจากฟังก์ชันที่ชื่อ “get_version()” ซึ่งรับพารามิเตอร์เป็นรูปแบบนิพจน์ปกติ (regular expression หรือ regex) สำหรับแต่ละกระบวนการที่มี socket รอฟัง (listening socket) โดยฟังก์ชันนี้จะตรวจสอบว่าไบนารี่ที่เกี่ยวข้องกับกระบวนการตรงกับรูปแบบที่กำหนดหรือไม่ และถ้าตรงก็จะเรียกคำสั่งตรวจสอบเวอร์ชันของบริการนั้นๆ

Maxime Thiebaut ได้อธิบายถึงช่องโหว่โดยละเอียดว่า:

“แม้ว่าฟังก์ชันนี้จะทำงานได้ถูกต้องกับไบนารี่ของระบบ (เช่น /usr/bin/httpd) แต่การใช้คลาสอักขระ \S ที่จับตัวอักษรที่ไม่ใช่ช่องว่างอย่างกว้างในหลายๆ รูปแบบ regex ก็จับคู่กับไบนารี่ที่ไม่ใช่ของระบบได้เช่นกัน (เช่น /tmp/httpd)”

เนื่องจากไบนารี่ที่ไม่ใช่ของระบบเหล่านี้อยู่ในไดเรกทอรี (เช่น /tmp) ซึ่งโดยปกติแล้วจะให้ผู้ใช้ที่ไม่ใช่แอดมินสามารถเขียนไฟล์ได้

ผลลัพธ์คือ: ช่องโหว่นี้เปิดทางให้ผู้โจมตีภายในเครื่องซึ่งไม่มีสิทธิ์ยกระดับความสามารถได้ง่าย โดยการวางไบนารี่ประสงค์ร้ายไว้ที่ “/tmp/httpd” แล้วเมื่อบริการเก็บข้อมูลเมตริกของ VMware ถูกเรียกใช้ ก็จะถูกยกระดับสิทธิ์ขึ้นมาโดยอัตโนมัติ ดังนั้นผู้โจมตีเพียงแค่ทำให้ไบนารี่ดังกล่าวถูกรันโดยผู้ใช้ที่ไม่มีสิทธิ์และเปิด socket ที่สุ่มขึ้นมาเท่านั้นก็เพียงพอ

```
get_version() {
  PATTERN=$1
  VERSION_OPTION=$2
  for p in $space_separated_pids
  do
    COMMAND=$(get_command_line $p | grep -Eo "$PATTERN")
    [ ! -z "$COMMAND" ] && echo VERSIONSTART "$p" "$("${COMMAND%%[[:space:]]*}" $VERSION_OPTION 2>&1)"
  done
}
```

หลักฐานการโจมตีและการเชื่อมโยงกับ UNC5174

บริษัทจากบรัสเซลส์รายนี้สังเกตว่าได้เห็น UNC5174 ใช้ตำแหน่ง “/tmp/httpd” เพื่อวางไบนารี่ประสงค์ร้าย, สร้าง shell ที่ยกระดับเป็น root และทำให้สามารถรันโค้ดในสิทธิ์สูงได้ อย่างไรก็ตามรายละเอียดของ payload ที่ถูกรันยังไม่ชัดเจนในขณะนี้ โดย NVISO Labs ให้เหตุผลว่าได้ตัดสินใจที่จะไม่เผยแพร่รายละเอียดเพิ่มเติมเกี่ยวกับ payload ที่ใช้หลังจากการใช้ประโยชน์จาก CVE-2025-41244 ในตอนนี้

Thiebaut กล่าวถึงนัยยะที่กว้างขึ้นของการโจมตีนี้: “การปฏิบัติทั่วไปที่เลียนแบบไบนารี่ของระบบ (เช่น httpd) ชี้ให้เห็นเป็นไปได้จริงว่า มัลแวร์หลายสายพันธุ์อาจบังเอิญได้รับผลประโยชน์จากการยกระดับสิทธิ์ที่ไม่ได้ตั้งใจมานานหลายปีแล้ว”

คำแนะนำและการแก้ไข

VMware Tools 12.4.9 ซึ่งอยู่ในชุด VMware Tools 12.5.4 ได้แก้ไขปัญหาสำหรับระบบ Windows 32-bit แล้ว และเวอร์ชันของ open-vm-tools ที่แก้ไข CVE-2025-41244 จะถูกแจกจ่ายโดยผู้จำหน่าย Linux ต่างๆ ผู้ใช้ควรเร่งดำเนินการอัปเดตเพื่อป้องกันการยกระดับสิทธิ์ที่อาจเกิดขึ้นตามมาจากการถูกโจมตีครั้งก่อน

ข้อมูลอ้างอิง

Sep 30, 2025, By Ravie Lakshmanan

- https://thehackernews.com/2025/09/urgent-china-linked-hackers-exploit-new.html