แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ

- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : CLEAR



ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

ช่องโหว่ Critical ในผลิตภัณฑ์ HP ArubaOS หลายรายการ เสี่ยงถูกใช้ในการโจมตี

วันที่แจ้งเตือน 30 ตุลาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ThaiCERT สกมช. ได้ติดตามสถานการณ์ภัยคุกคามทางไซเบอร์กรณีพบรายงานช่องโหว่ด้านความมั่นคงปลอดภัยในระบบปฏิบัติการ HP Aruba Operating System (ArubaOS หรือ AOS) ซึ่งใช้สำหรับบริหารจัดการโครงสร้างพื้นฐานเครือข่ายไร้สายระดับองค์กร (Enterprise Networking and Security) มีช่องโหว่ทั้งหมด 72 รายการ โดยเป็นช่องโหว่ระดับ Critical จำนวน 8 รายการ (คะแนน CVSS 10.0) ซึ่งอาจเปิดโอกาสให้ผู้ไม่หวังดีสามารถข้ามกระบวนการยืนยันตัวตน (Authentication Bypass) หรือสั่งรันคำสั่งบนระบบ (Remote Code Execution: RCE) ได้โดยไม่จำเป็นต้องมีสิทธิเข้าถึงหรือการโต้ตอบจากผู้ใช้งาน

ช่องโหว่ และ ผลกระทบ

CVE	ผลิตภัณฑ์	ประเภทช่องโหว่	ผลกระทบ
CVE-2026-79844	AOS-10	Authentication Bypass	ข้ามการยืนยันตัวตนและนำไปสู่ Remote Code Execution
CVE-2026-79845	AOS-10 / PAPI	Authentication Bypass	เข้าถึงสิทธิ Admin เปลี่ยน Configuration และเข้าถึง/แก้ไขข้อมูลสำคัญ
CVE-2026-79846	AOS-8	Command Injection	ผู้ไม่หวังดีที่ไม่ต้องยืนยันตัวตน อาจรันคำสั่งบนระบบปฏิบัติการ
CVE-2026-79847	AOS-10	Buffer Overflow	Remote Code Execution ด้วยสิทธิระดับสูง
CVE-2026-79848	AOS-8	SQL Injection	SQL Injection ที่สามารถนำไปสู่การรันคำสั่งบน OS
CVE-2026-79849	AOS-8	SQL Injection	SQL Injection ที่สามารถนำไปสู่การรันคำสั่งบน OS
CVE-2026-79850	AOS-8	Authentication Bypass	รันคำสั่งด้วยสิทธิ root และอาจยึดระบบทั้งหมด
CVE-2026-79851	AOS-10	Buffer Overflow	Remote Code Execution ด้วยสิทธิสูงและอาจยึดระบบทั้งหมด

แนวทางการป้องกันและรับมือ:

1. ตรวจสอบเวอร์ชันของ ArubaOS บนอุปกรณ์และระบบบริหารจัดการเครือข่ายทั้งหมด โดยเฉพาะAOS-8 และ AOS-10 พร้อมเปรียบเทียบกับรายการเวอร์ชันที่ได้รับผลกระทบตามประกาศความปลอดภัยของ HPE
2. เร่งดำเนินการอัปเดต ArubaOS เป็นเวอร์ชันที่ได้รับการแก้ไขช่องโหว่แล้ว ตามคำแนะนำของ HPE โดยให้ความสำคัญกับอุปกรณ์ที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือเครือข่ายที่ไม่น่าเชื่อถือ
3. จำกัดการเข้าถึงช่องทางบริหารจัดการระบบ ทั้ง Command Line Interface (CLI) และ Web Management Interface โดยอนุญาตเฉพาะผู้ดูแลระบบและเครือข่ายที่ได้รับอนุญาต
4. แยกเครือข่ายสำหรับบริหารจัดการอุปกรณ์ออกจากเครือข่ายผู้ใช้งานทั่วไป โดยใช้ Management VLAN หรือเครือข่ายเฉพาะสำหรับการบริหารจัดการและกำหนดนโยบาย Firewall เพื่อควบคุมการเข้าถึง
5. ตรวจสอบ Logs ของอุปกรณ์ ArubaOS, Firewall และระบบ SIEM เพื่อค้นหาความพยายามเข้าถึงระบบโดยไม่ได้รับอนุญาต การเปลี่ยนแปลงการตั้งค่าที่ผิดปกติ และกิจกรรมต้องสงสัยที่อาจเกี่ยวข้องกับการโจมตี
6. สำรองข้อมูลการตั้งค่าของอุปกรณ์ก่อนดำเนินการอัปเดต พร้อมตรวจสอบความพร้อมของระบบและทดสอบการทำงานหลังติดตั้งแพตช์ เพื่อป้องกันผลกระทบต่อการให้บริการเครือข่าย

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 30 ต.ค. 2569
2. https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05162en_us&docLocale=en_US

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ