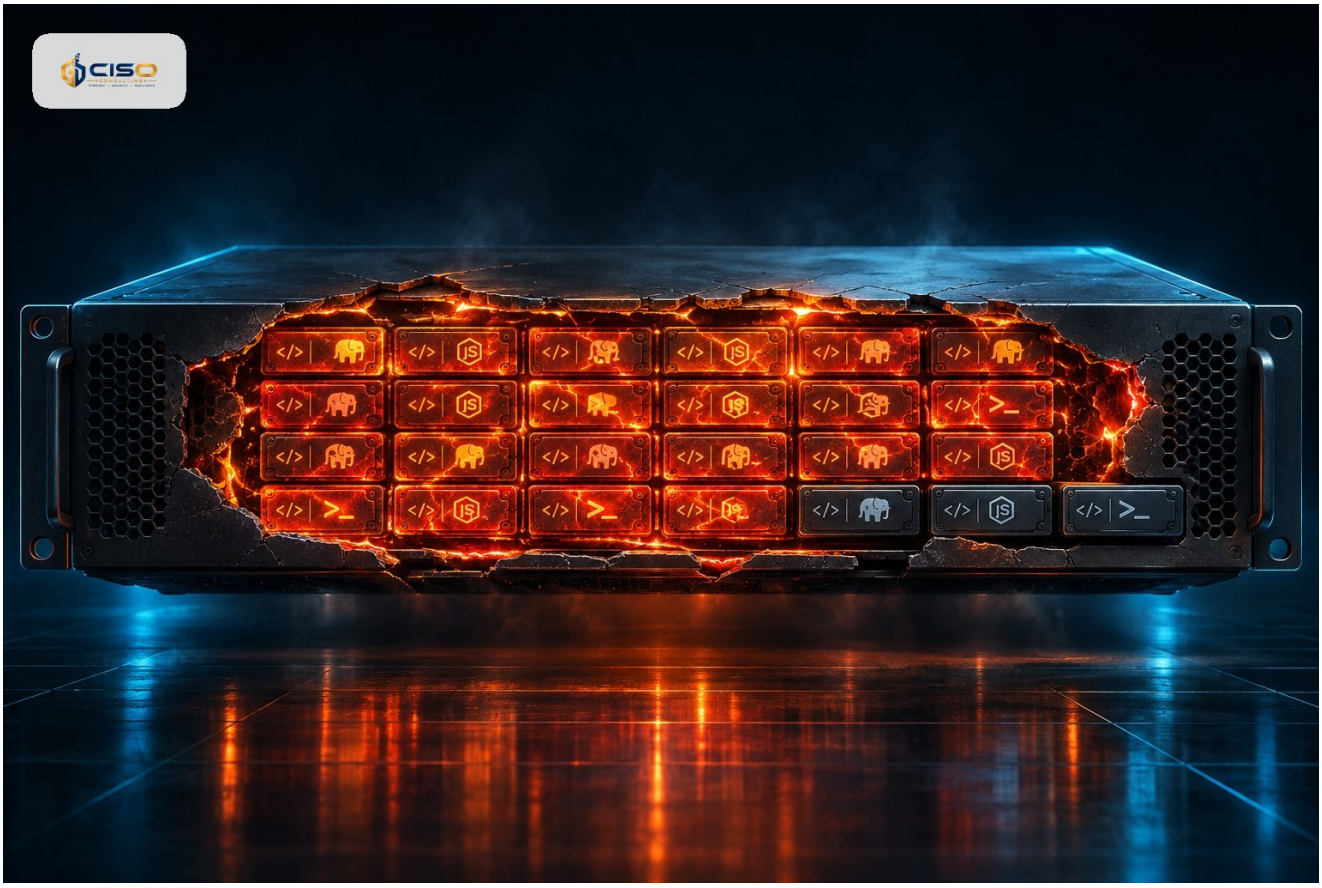
InfraTrust: معظم الثغرات المستغلة في الأجهزة تأتي من مكوّنات خارجية مدمجة



يفيد تقرير InfraTrust من Eclypsium لشهر نوفمبر بأن 33 من 38 نشرة أمنية عن ثغرات مستغلة تتعلق بمكوّنات مدمجة مثل PHP وNode.js وOpenSSH، ويحدد أولويات التحديث وإجراءات التحصين.

- يغطي التقرير 373 نشرة أمنية من 23 مورّد بنية تحتية بين 15 أكتوبر و19 نوفمبر، تضم 3,880 ثغرة، منها 98 نشرة بدرجة حرجة.
- تضمنت 38 نشرة ثغرات مدرجة في كتالوج KEV التابع لـCISA، وتتعلق 33 منها بمكوّنات مدمجة، أبرزها PHP وNode.js وOpenSSH.
- تُستغل ثغرتا PHP2Shell (CVE-2026-109618) وCVE-2026-109619) ضد جدران Palo Alto Networks وCheck Point، وكانت الإصلاحات لدى عدة موردين أخرى جزئية أو غير متاحة حتى 20 نوفمبر.
- تشمل أولويات التحديث Cisco Expressway وبوابات Check Point وArista VeloCloud

Orchestrator وCisco ASA وFTD وSonicOS SonicWall.

- توصي InfraTrust بإزالة واجهات الإدارة من الإنترنت وعزلها داخليًا وفحص الأجهزة التي سبق تعرضها بحثًا عن أبواب خلفية.

يشير تقرير InfraTrust Pulse لشهر نوفمبر من Eclypsium إلى أن التعرض للثغرات المستغلة في أجهزة الشبكات يعتمد بشكل متزايد على برمجيات لم يطورها المورّدون أنفسهم.

ما الذي رصده التقرير

تتبع التقرير بين 15 أكتوبر و19 نوفمبر 373 نشرة أمنية من 23 مورّدًا للبنية التحتية. ومن بين 38 نشرة تضمنت ثغرات مدرجة في كتالوج KEV التابع لـCISA، عالجت 33 منها ثغرات في مكوّنات مدمجة، أبرزها PHP وNode.js وOpenSSH. وحتى بعد صدور الإصلاح من المطوّر الأصلي، ينتظر العملاء إعادة المورّد بناء منتجه.

وتوضح ثغرتا PHP2Shell (CVE-2026-109618 وCVE-2026-109619) المشكلة؛ إذ تُستغلان ضد جدران Palo Alto Networks وCheck Point، وتُسلسلان مع ثغرات أخرى للحصول على صلاحيات الجذر. وأفادت Check Point بهجمات تدميرية نشرت برمجيات مسح بيانات على مضيفات VMware ESXi. وحتى 20 نوفمبر كانت الإصلاحات لمنتجات Fortinet وJuniper وLenovo وHPE وNetgear وHP وSiemens جزئية أو لم تصدر بعد.

تحديثات ذات أولوية

تشير InfraTrust إلى CVE-2026-76466 (Cisco Expressway)، وثغرتي PHP2Shell وCVE-2026-123039 في بوابات Check Point، وCVE-2026-114625 (Arista VeloCloud Orchestrator)، وCisco Secure Firewall ASA وFTD (CVE-2026-76418))، وCVE-2026-19868 (SonicWall SonicOS)، كما توصي بتحديثات Fortinet التحصينية الصادرة في أكتوبر.

قبل الإصلاح وبعده

نظرًا لتأخر الإصلاحات، ينصح التقرير بإزالة واجهات الإدارة من الإنترنت، وعزلها داخليًا للحد من الحركة الجانبية، وفحص الأجهزة التي سبق تعرضها، فقد تبقى الأبواب الخلفية بعد التحديث.

ما يجب فعله الآن

1. طابق سجل جدران الحماية وشبكات VPN والبوابات لديك مع المنتجات والثغرات المذكورة، وابدأ بتحديث المستغلة منها.
2. اطلب من كل مورّد حالة إصلاحات PHP2Shell وPHP وNode.js وOpenSSH ووثّق الردود.
3. أزل واجهات إدارة الأجهزة من الإنترنت وقصرها على شبكات إدارية معزولة.
4. افحص الأجهزة التي سبق تعرضها بحثًا عن أبواب خلفية أو آليات بقاء حتى لو جرى تحديثها.
5. أدرج المكوّنات الخارجية المدمجة وجداول إعادة بناء المورّدين ضمن مراجعات مخاطر الأطراف الثالثة وإدارة الثغرات.