Scottish Cyber Coordination Centre

Daily threat bulletin

8 November 2024

Vulnerabilities

CISA warns of critical Palo Alto Networks bug exploited in attacks

BleepingComputer - 07 November 2024 15:03

Today, CISA warned that attackers are exploiting a critical missing authentication vulnerability in Palo Alto Networks Expedition, a migration tool that can help convert firewall configuration from Checkpoint, Cisco, and other vendors to PAN-OS. [...]

HPE warns of critical RCE flaws in Aruba Networking access points

BleepingComputer - 07 November 2024 11:47

Hewlett Packard Enterprise (HPE) released updates for Instant AOS-8 and AOS-10 software to address two critical vulnerabilities in Aruba Networking Access Points. [...]

Cisco Patches Critical Vulnerability in Industrial Networking Solution

SecurityWeek - 07 November 2024 13:24

A critical vulnerability in Cisco Unified Industrial Wireless software could allow remote, unauthenticated attackers to inject commands with root privileges.

CISA Adds Four Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added four new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. CVE-2024-43093 Android Framework Privilege Escalation Vulnerability. CVE-2024-51567 CyberPanel Incorrect Default Permissions Vulnerability. CVE-2019-16278 Nostromo nhttpd Directory Traversal Vulnerability. CVE-2024-5910 Palo Alto Expedition Missing Authentication Vulnerability.

Threat actors and malware

DPRK-linked BlueNoroff used macOS malware with novel persistence

Security Affairs - 07 November 2024 17:16

SentinelLabs observed North Korea-linked threat actor BlueNoroff targeting businesses in the crypto industry with a new multi-stage malware. SentinelLabs researchers identified a North Korea-linked threat actor targeting crypto businesses with new macOS malware as part of a campaign tracked as “Hidden Risk.”

New CRON#TRAP Malware Infects Windows by Hiding in Linux VM to Evade Antivirus

Scottish Cyber Coordination Centre

The Hacker News - 08 November 2024 13:45

Cybersecurity researchers have flagged a new malware campaign that infects Windows systems with a Linux virtual instance containing a backdoor capable of establishing remote access to the compromised hosts.The “intriguing” campaign, codenamed CRON#TRAP, starts with a malicious Windows shortcut (LNK) file likely distributed in the form of a ZIP archive via a phishing email.

‘SteelFox’ Malware Blitz Infects 11K Victims With Bundle of Pain

darkreading - 07 November 2024 20:40

The malware combines a miner and data stealer, and it packs functions that make detection and mitigation a challenge.

Android Banking Trojan ToxicPanda Targets Europe

SecurityWeek - 07 November 2024 10:40

ToxicPanda is a China-linked Android banking trojan spotted targeting over a dozen banks in Europe and Latin America.