Daily threat bulletin

27 September 2024

Vulnerabilities

CUPS flaws enable Linux remote code execution, but there’s a catch

BleepingComputer - 26 September 2024 19:03

Under certain conditions, attackers can chain a set of vulnerabilities in multiple components of the CUPS open-source printing system to execute arbitrary code remotely on vulnerable machines. [...]

Critical RCE vulnerability found in OpenPLC

Security Affairs - 26 September 2024 18:49

Cisco’s Talos reported critical and high-severity flaws in OpenPLC that could lead to DoS condition and remote code execution. Cisco’s Talos threat intelligence unit has disclosed details of five newly patched vulnerabilities in OpenPLC, an open-source programmable logic controller.

Security Upgrades Available for 3 HPE Aruba Networking Bugs

darkreading - 26 September 2024 21:15

The vendor says there are no reports of the flaws being exploited in the wild nor any public exploit codes currently available.

Patch now: Critical Nvidia bug allows container escape, complete host takeover

The Register - 26 September 2024 22:42

33% of cloud environments using the toolkit impacted, we’re told A critical bug in Nvidia’s widely used Container Toolkit could allow a rogue user or software to escape their containers and ultimately take complete control of the underlying host.

Cisco Patches High-Severity Vulnerabilities in IOS Software

SecurityWeek - 26 September 2024 13:47

Cisco has released patches for seven high-severity vulnerabilities affecting products running IOS and IOS XE software.

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation - CVE-2024-7593 Ivanti Virtual Traffic Manager Authentication Bypass Vulnerability.

Versa Networks Releases Advisory for a Vulnerability in Versa Director, CVE-2024-45229

CISA Advisories -

Versa Networks has released an advisory for a vulnerability (CVE-2024-45229) affecting Versa Director. A cyber threat actor could exploit this vulnerability to exercise unauthorized REST APIs.

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation - CVE-2024-8963 Ivanti Cloud Services Appliance (CSA) Path Traversal Vulnerability.

Threat actors and malware

Ransomware on the rise: Healthcare industry attack trends 2024

Security Intelligence - 26 September 2024 14:00

According to the IBM Cost of a Data Breach Report 2024, the global average cost of a data breach reached $4.88 million this year, a 10% increase over 2023. For the healthcare industry, the report offers both good and bad news.

UK related

Police Are Probing a Cyberattack on Wi-Fi Networks at UK Train Stations

SecurityWeek - 26 September 2024 12:45

An investigation has been launched into a Wi-Fi service hack that has impacted many train stations in the United Kingdom.The post Police Are Probing a Cyberattack on Wi-Fi Networks at UK Train Stations appeared first on SecurityWeek.