Scottish Cyber Coordination Centre

Daily threat bulletin

3 October 2024

Vulnerabilities

Critical Ivanti RCE flaw with public exploit now used in attacks

BleepingComputer - 02 October 2024 15:55

CISA warned today that a critical Ivanti vulnerability that can let threat actors gain remote code execution on vulnerable Endpoint Manager (EPM) appliances is now actively exploited in attacks. [...]

DrayTek fixed critical flaws in over 700,000 exposed routers

BleepingComputer - 02 October 2024 10:00

DrayTek has released security updates for multiple router models to address 14 vulnerabilities of varying severity, including a remote code execution flaw that received the maximum CVSS score of 10. [...]

Alert: Adobe Commerce and Magento Stores Under Attack from CosmicSting Exploit

The Hacker News - 02 October 2024 18:43

Cybersecurity researchers have disclosed that 5% of all Adobe Commerce and Magento stores have been hacked by malicious actors by exploiting a security vulnerability dubbed CosmicSting.Tracked as CVE-2024-34102 (CVSS score: 9.8), the critical flaw relates to an improper restriction of XML external entity reference (XXE) vulnerability that could result in remote code execution.

Two simple give-me-control security bugs found in Optigo network switches used in critical manufacturing

The Register - 02 October 2024 21:39

Poor use of PHP include() strikes again Two trivial but critical security holes have been found in Optigo’s Spectra Aggregation Switch, and so far no patch is available.

Critical Zimbra Vulnerability Exploited One Day After PoC Release

SecurityWeek - 02 October 2024 09:48

A critical-severity vulnerability in Zimbra has been exploited in the wild to deploy a web shell on vulnerable servers.The post Critical Zimbra Vulnerability Exploited One Day After PoC Release appeared first on SecurityWeek.

Threat actors and malware

FIN7 hackers launch deepfake nude “generator” sites to spread malware

BleepingComputer - 02 October 2024 17:01

The notorious APT hacking group known as FIN7 launched a network of fake AI-powered deepnude generator sites to infect visitors with information-stealing malware. [...]

Fake browser updates spread updated WarmCookie malware

BleepingComputer - 02 October 2024 15:22

A new ‘FakeUpdate’ campaign targeting users in France leverages compromised websites to show fake browser and application updates that spread a new version of the WarmCookie malware. [...]

Andariel Hacking Group Shifts Focus to Financial Attacks on U.S. Organizations

The Hacker News - 02 October 2024 16:30

Three different organizations in the U.S. were targeted in August 2024 by a North Korean state-sponsored threat actor called Andariel as part of a likely financially motivated attack.

Fake Trading Apps Target Victims Globally via Apple App Store and Google Play

The Hacker News - 02 October 2024 23:24

A large-scale fraud campaign leveraged fake trading apps published on the Apple App Store and Google Play Store, as well as phishing sites, to defraud victims, per findings from Group-IB.

Stonefly Group Targets US Firms With New Malware Tools

Infosecurity Magazine - 02 October 2024 16:30

North Korean APT Stonefly continues to launch cyber-attacks on US firms despite July indictment.

MITRE Adds Mitigations to EMB3D Threat Model

SecurityWeek - 02 October 2024 14:01

MITRE has expanded the EMB3D Threat Model with essential mitigations to help organizations address threats to embedded devices.

UK related

Hackers pose as British postal carrier to deliver Prince ransomware in destructive campaign

The Record from Recorded Future News - 02 October 2024 19:13

Researchers have identified a new campaign in which hackers impersonated the British postal carrier Royal Mail to target victims in the U.S. and the U.K. with Prince ransomware.

Northern Ireland police fined for data breach exposing secret identities of officers

The Record from Recorded Future News - 03 October 2024 00:01

The Police Service of Northern Ireland (PSNI) has been fined £750,000 ($1 million) by the United Kingdom's data protection regulator after accidentally revealing the identities of all of its officers and staff, potentially exposing them to terrorist and criminal groups and "leaving many fearing for their safety."