Scottish Cyber Coordination Centre

Daily threat bulletin

20 December 2024

Vulnerabilities

Fortinet warns of FortiWLM bug giving hackers admin privileges

BleepingComputer - 19 December 2024 13:24

Fortinet has disclosed a critical vulnerability in Fortinet Wireless Manager (FortiWLM) that allows remote attackers to take over devices by executing unauthorized code or commands through specially crafted web requests. [...]

Orgs Scramble to Fix Actively Exploited Bug in Apache Struts 2

darkreading - 19 December 2024 18:46

A newly discovered vulnerability, CVE-2024-53677, in the aging Apache framework is going to cause major headaches for IT teams, since patching isn't enough to fix it.

Chrome 131 Update Patches High-Severity Memory Safety Bugs

SecurityWeek - 19 December 2024 12:31

Google has released a Chrome 131 update to patch multiple high-severity memory safety vulnerabilities, including three affecting the V8 JavaScript engine.

Vulnerability Exploit Assessment Tool EPSS Exposed to Adversarial Attack

Infosecurity Magazine - 19 December 2024 11:30

A Morphisec researcher showed how an attacker could manipulate FIRST's Exploit Prediction Scoring System (EPSS) using AI

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-2024-12356 BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) Command Injection Vulnerability.

Threat actors and malware

BadBox malware botnet infects 192,000 Android devices despite disruption

BleepingComputer - 19 December 2024 18:01

The BadBox Android malware botnet has grown to over 192,000 infected devices worldwide despite a recent sinkhole operation that attempted to disrupt the operation in Germany. [...]

Scottish Cyber Coordination Centre

Android malware found on Amazon Appstore disguised as health app

BleepingComputer - 19 December 2024 14:59

A malicious Android spyware application named 'BMI CalculationVsn' was discovered on the Amazon Appstore, masquerading as a simple health tool but stealing data from infected devices in the background. [...]

Juniper Warns of Mirai Botnet Targeting SSR Devices with Default Passwords

The Hacker News - 19 December 2024 20:07

Juniper Networks is warning that Session Smart Router (SSR) products with default passwords are being targeted as part of a malicious campaign that deploys the Mirai botnet malware.

OT/ICS Engineering Workstations Face Barrage of Fresh Malware

darkreading - 19 December 2024 23:45

Cyberattacks against OT/ICS engineering workstations are widely underestimated, according to researchers who discovered malware designed to shut down Siemens workstation engineering processes.

Black Friday chaos: The return of Gozi malware

Security Intelligence - 19 December 2024 12:00

On November 29th, 2024, Black Friday, shoppers flooded online stores to grab the best deals of the year. But while consumers were busy filling their carts, cyber criminals were also seizing the opportunity to exploit the shopping frenzy.