



Daily threat bulletin

5 December 2024

Vulnerabilities

[Veeam Issues Patch for Critical RCE Vulnerability in Service Provider Console](#)

The Hacker News - 04 December 2024 12:04

Veeam has released security updates to address a critical flaw impacting Service Provider Console (VSPC) that could pave the way for remote code execution on susceptible instances. The vulnerability, tracked as CVE-2024-42448, carries a CVSS score of 9.9 out of a maximum of 10.0.

[Japan warns of IO-Data zero-day router flaws exploited in attacks](#)

BleepingComputer - 04 December 2024 11:28

Japan's CERT is warning that hackers are exploiting zero-day vulnerabilities in I-O Data router devices to modify device settings, execute commands, or even turn off the firewall. [...]

[Android's December 2024 Security Update Patches 14 Vulnerabilities](#)

SecurityWeek - 04 December 2024 12:59

Google has released patches for 14 high-severity vulnerabilities as part of Android's December 2024 security update.

[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-2024-51378 CyberPanel Incorrect Default Permissions Vulnerability. These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise.

Threat actors and malware

[New DroidBot Android malware targets 77 banking, crypto apps](#)

BleepingComputer - 04 December 2024 14:26

A new Android banking malware named 'DroidBot' attempts to steal credentials for over 77 cryptocurrency exchanges and banking apps in the UK, Italy, France, Spain, and Portugal. [...]

[CISA Issues Guidance to Telecom Sector on Salt Typhoon Threat](#)

darkreading - 04 December 2024 23:06



Scottish
Cyber
Coordination
Centre

Individuals concerned about the privacy of their communications should consider using encrypted messaging apps and encrypted voice communications, CISA and FBI officials say.

ENISA Launches First State of EU Cybersecurity Report

Infosecurity Magazine - 04 December 2024 14:00

The NIS2 directive requires the EU cybersecurity agency to produce a biennial report on the state of cybersecurity in the Union

Spy v Spy: Russian APT Turla Caught Stealing From Pakistani APT

SecurityWeek - 04 December 2024 18:00

Russia's Turla hackers hijacked 33 command servers operated by Pakistani hackers who had themselves breached Afghanistan and Indian targets.

UK related

British telecoms giant BT confirms attempted cyberattack after ransomware gang claims hack

The Record from Recorded Future News - 04 December 2024 19:14

UK disrupts Russian money laundering networks used by ransomware

BleepingComputer - 04 December 2024 16:18

A law enforcement operation led by the United Kingdom's National Crime Agency (NCA) has disrupted two Russian money laundering networks working with criminals worldwide, including ransomware gangs. [...]