Scottish Cyber Coordination Centre

Daily threat bulletin

20 January 2025

Vulnerabilities

A flaw in the W3 Total Cache plugin exposes hundreds of thousands of WordPress sites to attacks

Security Affairs - 19 January 2025 20:20

A WordPress W3 Total Cache plugin vulnerability could allow attackers to access information from internal services, including metadata on cloud-based apps. A severe vulnerability, tracked as CVE-2024-12365 (CVSS score of 8.5) in the WordPress W3 Total Cache plugin could expose metadata from internal services and cloud apps.

Critical Flaws in WGS-804HPT Switches Enable RCE and Network Exploitation

The Hacker News - 17 January 2025 20:38

Cybersecurity researchers have disclosed three security flaws in Planet Technology's WGS-804HPT industrial switches that could be chained to achieve pre-authentication remote code execution on susceptible devices.

Six vulnerabilities in ubiquitous rsync tool announced and fixed in a day

The Register - 17 January 2025 16:49

Turns out tool does both file transfers and security fixes fast Don't panic. Yes, there were a bunch of CVEs, affecting potentially hundreds of thousands of users, found in rsync in early December.

ESET detailed a flaw that could allow a bypass of the Secure Boot in UEFI systems

Security Affairs - 17 January 2025 12:15

Researchers detailed a now-patched vulnerability that could allow a bypass of the Secure Boot mechanism in UEFI systems. ESET disclosed details of a now-patched vulnerability, tracked as CVE-2024-7344 (CVSS score: 6.7), that could allow a bypass of the Secure Boot mechanism in UEFI systems.

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-2024-50603 Aviatrix Controllers OS Command Injection Vulnerability.

Threat actors and malware

Scottish Cyber Coordination Centre

New 'Sneaky 2FA' Phishing Kit Targets Microsoft 365 Accounts with 2FA Code Bypass

The Hacker News - 17 January 2025 16:37

Cybersecurity researchers have detailed a new adversary-in-the-middle (AitM) phishing kit that's capable of Microsoft 365 accounts with an aim to steal credentials and two-factor authentication (2FA) codes since at least October 2024.

Star Blizzard hackers abuse WhatsApp to target high-value diplomats

BleepingComputer - 19 January 2025 11:23

Russian nation-state actor Star Blizzard has been running a new spear-phishing campaign to compromise WhatsApp accounts of targets in government, diplomacy, defense policy, international relations, and Ukraine aid organizations. [...]

Lazarus Group Targets Developers in New Data Theft Campaign

Infosecurity Magazine - 17 January 2025 16:30

SecurityScorecard identified a new campaign in which the North Korean Lazarus group aims to steal source code, secrets and cryptocurrency wallet keys from developer environments

UK related

Medusa ransomware group claims attack on UK's Gateshead Council

The Register - 17 January 2025 11:30

Pastes allegedly stolen documents on leak site with £600K demand.

Cyber Essentials NHS and Healthcare Organisations

Security Boulevard - 18 January 2025 15:57

What is Cyber Essentials? Cyber Essentials scheme is a UK government-backed initiative designed to help organisations, large or small, shield themselves from common cyber threats. It outlines a straightforward set of technical security controls that, when appropriately implemented, can reduce an organisation's attack surface.