Scottish Cyber Coordination Centre

Daily threat bulletin

16 January 2025

Vulnerabilities

Researcher Uncovers Critical Flaws in Multiple Versions of Ivanti Endpoint Manager

The Hacker News - 16 January 2025 13:09

Ivanti has rolled out security updates to address several security flaws impacting Avalanche, Application Control Engine, and Endpoint Manager (EPM), including four critical bugs that could lead to information disclosure.

SAP fixes critical vulnerabilities in NetWeaver application servers

BleepingComputer - 15 January 2025 18:02

SAP has fixed two critical vulnerabilities affecting NetWeaver web application server that could be exploited to escalate privileges and access restricted information. [...]

U.S. CISA adds Fortinet FortiOS to its Known Exploited Vulnerabilities catalog

Security Affairs - 15 January 2025 15:58

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added a Fortinet FortiOS authorization bypass vulnerability, tracked as CVE-2024-55591 (CVSS score: 9.6) to its Known Exploited Vulnerabilities (KEV) catalog.

CVE-2024-44243 macOS flaw allows persistent malware installation

Security Affairs - 15 January 2025 11:34

Microsoft disclosed details of a vulnerability in Apple macOS that could have allowed an attacker to bypass the OS's System Integrity Protection (SIP). Microsoft disclosed details of a now-patched macOS flaw, tracked as CVE-2024-44243 (CVSS score: 5.5), that allows attackers with "root" access to bypass System Integrity Protection (SIP).

Windows BitLocker bug triggers warnings on devices with TPMs

BleepingComputer - 15 January 2025 11:46

Microsoft is investigating a bug triggering security alerts on systems with a Trusted Platform Module (TPM) processor after enabling BitLocker. [...]

Nvidia, Zoom, Zyxel Patch High-Severity Vulnerabilities

SecurityWeek - 15 January 2025 13:59

Nvidia, Zoom, and Zyxel have released patches for multiple high-severity vulnerabilities across their products.

Scottish Cyber Coordination Centre

Threat actors and malware

Threat actor leaked config files and VPN passwords for over Fortinet Fortigate devices

Security Affairs - 16 January 2025 01:03

A previously unknown threat actor released config files and VPN passwords for Fortinet FortiGate devices on a popular cybercrime forum. A previously unknown threat actor named Belsen Group published configuration files and VPN passwords for over 15,000 Fortinet FortiGate appliances. “2025 will be a fortunate year for the world.

MikroTik botnet uses misconfigured SPF DNS records to spread malware

BleepingComputer - 15 January 2025 16:04

A newly discovered botnet of 13,000 MikroTik devices uses a misconfiguration in domain name server records to bypass email protections and deliver malware by spoofing roughly 20,000 web domains. […]

Google Ads Users Targeted in Malvertising Scam Stealing Credentials and 2FA Codes

The Hacker News - 15 January 2025 22:18

Cybersecurity researchers have alerted to a new malvertising campaign that’s targeting individuals and businesses advertising via Google Ads by attempting to phish for their credentials via fraudulent ads on Google.

Over 660,000 Rsync servers exposed to code execution attacks

BleepingComputer - 15 January 2025 13:00

Over 660,000 exposed Rsync servers are potentially vulnerable to six new vulnerabilities, including a critical-severity heap-buffer overflow flaw that allows remote code execution on servers. […]

Codefinger ransomware gang uses compromised AWS keys to encrypt S3 bucket

Security Affairs - 15 January 2025 12:53

The ransomware group Codefinger is using compromised AWS keys to encrypt S3 bucket data using SSE-C, Halcyon researchers warn. The ransomware group Codefinger has been spotted using compromised AWS keys to encrypt data in S3 buckets.

RansomHub Affiliate leverages Python-based backdoor

Security Boulevard - 15 January 2025 22:53

In an incident response in Q4 of 2024, GuidePoint Security identified evidence of a threat actor utilizing a Python-based backdoor […]