Scottish Cyber Coordination Centre

Daily Threat Bulletin

12 May 2025

Vulnerabilities

SonicWall fixed SMA 100 flaws that could be chained to execute arbitrary code

Security Affairs - 09 May 2025 08:50

SonicWall addressed three SMA 100 flaws, including a potential zero-day, that could allow remote code execution if chained. SonicWall patches three SMA 100 vulnerabilities (CVE-2025-32819, CVE-2025-32820, and CVE-2025-32821), including a potential zero-day, that could be chained by a remote attacker to execute arbitrary code.

Beyond Vulnerability Management – Can You CVE What I CVE?

The Hacker News - 09 May 2025 17:27

The reactive nature of vulnerability management, combined with delays from policy and process, strains security teams. Capacity is limited and patching everything immediately is a struggle.

Commvault: Vulnerability Patch Works as Intended

darkreading - 09 May 2025 17:58

The security researcher who questioned the effectiveness of a patch for recently disclosed bug in Commvault Command Center did not test patched version, the company says.

Threat actors and malware

Chinese hackers behind attacks targeting SAP NetWeaver servers

BleepingComputer - 09 May 2025 13:23

Forescout Vedere Labs security researchers have linked ongoing attacks targeting a maximum severity vulnerability impacting SAP NetWeaver instances to a Chinese threat actor. [...]

Cybercriminal services target end-of-life routers, FBI warns

Security Affairs - 09 May 2025 12:43

The FBI warns that attackers are using end-of-life routers to deploy malware and turn them into proxies sold on 5Socks and Anyproxy networks. The FBI released a FLASH alert warning about 5Socks and Anyproxy malicious services targeting end-of-life (EOL) routers. Attackers target EoL devices to deploy malware by exploiting vulnerabilities and create botnets for attacks [...]

Russia-linked ColdRiver used LostKeys malware in recent attacks

Scottish Cyber Coordination Centre

Security Affairs - 09 May 2025 09:41

Since early 2025, Russia-linked ColdRiver has used LostKeys malware to steal files in espionage attacks on Western governments and organizations. Google's Threat Intelligence Group discovered LOSTKEYS, a new malware used by Russia-linked APT COLDRIVER, in recent attacks to steal files and gather system info. The ColdRiver APT (aka "Seaborgium", "Callisto", "Star Blizzard", "TA446") is a Russian cyberespionage group [...]

Chinese Hackers Exploit SAP RCE Flaw CVE-2025-31324, Deploy Golang-Based SuperShell

The Hacker News - 09 May 2025 10:59

A China-linked unnamed threat actor dubbed Chaya_004 has been observed exploiting a recently disclosed security flaw in SAP NetWeaver.Forescout Vedere Labs, in a report published Thursday, said it uncovered a malicious infrastructure likely associated with the hacking group weaponizing CVE-2025-31324 (CVSS score: 10.0) since April 29, 2025.CVE-2025-31324 refers to a critical SAP NetWeaver flaw

LockBit Ransomware Gang Hacked, Operations Data Leaked

darkreading - 09 May 2025 20:03

Exposed data from LockBit's affiliate panel includes Bitcoin addresses, private chats with victim organizations, and user information such as credentials.

UK related

UK's Legal Aid Agency Experiences Cyberattack

Security Magazine - 09 May 2025 13:19

An executive agency of the UK's Ministry of Justice experienced a cyberattack.