Scottish Cyber Coordination Centre

Daily Threat Bulletin

17 November 2025

Vulnerabilities

Now-Patched Fortinet FortiWeb Flaw Exploited in Attacks to Create Admin Accounts

The Hacker News - 14 November 2025 15:30

Cybersecurity researchers are sounding the alert about an authentication bypass vulnerability in Fortinet Fortiweb Web Application Firewall (WAF) that could allow an attacker to take over admin accounts and completely compromise a device.

Critical CVE-2025-59367 flaw lets hackers access ASUS DSL routers remotely

Security Affairs - 14 November 2025 20:16

ASUS patched a critical auth-bypass flaw, tracked as CVE-2025-59367 (CVSS score of 9.3), in multiple DSL routers that allows remote, unauthenticated attackers to easily access unpatched devices.

Multiple Vulnerabilities in GoSign Desktop lead to Remote Code Execution

Security Affairs - 15 November 2025 22:40

Researchers found a critical vulnerability in GoSign Desktop: TLS Certificate Validation Disabled and Unsigned Update Mechanism. GoSign is an advanced and qualified electronic signature solution developed by Tinexta InfoCert S.p.A., used by public administrations, businesses, and professionals to manage approval workflows with traceability and security.

Imunify360 Vulnerability Could Expose Millions of Sites to Hacking

SecurityWeek - 14 November 2025 10:35

A vulnerability in ImunifyAV can be exploited for arbitrary code execution by uploading a malicious file to shared servers.

Threat actors and malware

CISA and Partners Release Advisory Update on Akira Ransomware

CISA Advisories -

Today, Cybersecurity and Infrastructure Security Agency (CISA), in collaboration with various partners, released an updated joint Cybersecurity Advisory, #StopRansomware: Akira Ransomware, to provide network defenders with the latest indicators of compromise, tactics, techniques, and procedures, and detection methods associated with Akira ransomware activity.

Scottish Cyber Coordination Centre

North Korean Hackers Turn JSON Services into Covert Malware Delivery Channels

The Hacker News - 15 November 2025 00:55

The North Korean threat actors behind the Contagious Interview campaign have once again tweaked their tactics by using JSON storage services to stage malicious payloads. The threat actors have recently resorted to utilizing JSON storage services like JSON Keeper, JSONsilo, and npoint.io to host and deliver malware from trojanized code projects, with the lure.

Decades-old 'Finger' protocol abused in ClickFix malware attacks

BleepingComputer - 15 November 2025 14:46

The decades-old "finger" command is making a comeback,, with threat actors using the protocol to retrieve remote commands to execute on Windows devices.

Iranian Hackers Launch 'SpearSpecter' Spy Operation on Defense & Government Targets

The Hacker News - 14 November 2025 21:10

The Iranian state-sponsored threat actor known as APT42 has been observed targeting individuals and organizations that are of interest to the Islamic Revolutionary Guard Corps (IRGC) as part of a new espionage-focused campaign.

Anthropic Says Claude AI Powered 90% of Chinese Espionage Campaign

SecurityWeek - 14 November 2025 09:22

A state-sponsored threat actor manipulated Claude Code to execute cyberattacks on roughly 30 organizations worldwide.

UK incidents

Clop claims it hacked 'the NHS.' Which bit? Your guess is as good as theirs

The Register - 14 November 2025 10:30

Cybercrime crew has ravaged multiple private organizations using Oracle EBS zero-day for months The UK's National Health Service (NHS) is investigating claims of a cyberattack by extortion crew Clop.

Checkout.com snubs hackers after data breach, to donate ransom instead

BleepingComputer - 14 November 2025 12:25

UK financial technology company Checkout announced that the ShinyHunters threat group has breached one of its legacy cloud storage systems and is now extorting the company for a ransom.