Scottish Cyber Coordination Centre

Daily Threat Bulletin

14 November 2025

Vulnerabilities

Fortinet FortiWeb flaw with public PoC exploited to create admin users

BleepingComputer - 13 November 2025 22:41

A Fortinet FortiWeb path traversal vulnerability is being actively exploited to create new administrative users on exposed devices without requiring authentication.

RCE flaw in ImunifyAV puts millions of Linux-hosted sites at risk

BleepingComputer - 13 November 2025 15:04

The ImunifyAV malware scanner for Linux server, used by tens of millions of websites, is vulnerable to a remote code execution vulnerability that could be exploited to compromise the hosting environment.

ChatGPT Vulnerability Exposed Underlying Cloud Infrastructure

SecurityWeek - 13 November 2025 16:40

A researcher found a way to exploit an SSRF vulnerability related to custom GPTs to obtain an Azure access token. The post ChatGPT Vulnerability Exposed Underlying Cloud Infrastructure appeared first on SecurityWeek.

CISA Updates Guidance on Patching Cisco Devices Targeted in China-Linked Attacks

SecurityWeek - 13 November 2025 16:05

Federal agencies have reported as ‘patched’ ASA or FTD devices running software versions vulnerable to attacks.The post CISA Updates Guidance on Patching Cisco Devices Targeted in China-Linked Attacks appeared first on SecurityWeek.

Threat actors and malware

Kraken ransomware benchmarks systems for optimal encryption choice

BleepingComputer - 13 November 2025 18:53

The Kraken ransomware, which targets Windows, Linux/VMware ESXi systems, is testing machines to check how fast it can encrypt data without overloading them.

Amazon alerts: advanced threat actor exploits Cisco ISE & Citrix NetScaler zero-days

Security Affairs - 13 November 2025 09:42

Amazon warns that an advanced threat actor exploited zero-days in Cisco ISE and Citrix NetScaler to deploy custom malware. Amazon’s threat intelligence researchers spotted an

advanced threat actor exploiting two previously undisclosed zero-day flaws in Cisco Identity Service Engine (ISE) and Citrix NetScaler ADC to deliver custom malware.

NHS Investigating Oracle EBS Hack Claims as Hackers Name Over 40 Alleged Victims

SecurityWeek - 13 November 2025 13:54

The UK's national healthcare system is working with the country's National Cyber Security Centre to investigate the incident.The post NHS Investigating Oracle EBS Hack Claims as Hackers Name Over 40 Alleged Victims appeared first on SecurityWeek.

Critical WatchGuard Firebox Vulnerability Exploited in Attacks

SecurityWeek - 13 November 2025 13:31

Tracked as CVE-2025-9242 (CVSS score of 9.3), the flaw leads to unauthenticated, remote code execution on vulnerable firewalls.The post Critical WatchGuard Firebox Vulnerability Exploited in Attacks appeared first on SecurityWeek.

CISA and Partners Release Advisory Update on Akira Ransomware

CISA Advisories -

Today, Cybersecurity and Infrastructure Security Agency (CISA), in collaboration with the Federal Bureau of Investigation, Department of Defense Cyber Crime Center, Department of Health and Human Services, and international 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.

UK related

NHS supplier ends probe into ransomware attack that contributed to patient death

The Register - 13 November 2025 12:13

Synnovis's 18-month forensic review of Qilin intrusion completed, now affected patients to be notified Synnovis has finally wrapped up its investigation into the 2024 ransomware attack that crippled pathology services across London, ending an 18-month effort to untangle what the NHS supplier describes as one of the most complex data reconstruction jobs it has ever faced.

NHS Investigating Oracle EBS Hack Claims as Hackers Name Over 40 Alleged Victims

SecurityWeek - 13 November 2025 13:54

The UK's national healthcare system is working with the country's National Cyber Security Centre to investigate the incident. The post NHS Investigating Oracle EBS Hack Claims as Hackers Name Over 40 Alleged Victims appeared first on SecurityWeek.