Scottish Cyber Coordination Centre

Daily Threat Bulletin

20 October 2025

Vulnerabilities

ConnectWise fixes Automate bug allowing AiTM update attacks

BleepingComputer - 17 October 2025 16:29

ConnectWise released a security update to address vulnerabilities, one of them with critical severity, in Automate product that could expose sensitive communications to interception and modification. [...]

Microsoft fixes Windows bug breaking localhost HTTP connections

BleepingComputer - 17 October 2025 10:58

Microsoft has fixed a known issue breaking HTTP/2 localhost (127.0.0.1) connections and IIS websites after installing recent Windows security updates. [...]

A critical WatchGuard Fireware flaw could allow unauthenticated code execution

Security Affairs - 17 October 2025 15:09

A critical WatchGuard Fireware vulnerability, tracked as CVE-2025-9242, could allow unauthenticated code execution. Researchers revealed details of a critical vulnerability, tracked as CVE-2025-9242 (CVSS score of 9.3), in WatchGuard Fireware.

'Highest Ever' Severity Score Assigned by Microsoft to ASP.NET Core Vulnerability

SecurityWeek - 17 October 2025 11:46

CVE-2025-55315 is an HTTP request smuggling bug leading to information leaks, file content tampering, and server crashes.

Vulnerabilities Allow Disruption of Phoenix Contact UPS Devices

SecurityWeek - 17 October 2025 09:30

An attacker can exploit the flaws to put devices into a permanent DoS condition that prevents remote restoration.

Gladinet Patches Exploited CentreStack Vulnerability

SecurityWeek - 17 October 2025 08:51

The unauthenticated local file inclusion bug allows attackers to retrieve the machine key and execute code remotely via a ViewState deserialization issue.

CISA Directs Federal Agencies to Mitigate Vulnerabilities in F5 Devices

CISA Advisories -

Scottish Cyber Coordination Centre

Today, CISA issued Emergency Directive ED 26-01: Mitigate Vulnerabilities in F5 Devices to direct Federal Civilian Executive Branch agencies to inventory F5 BIG-IP products, evaluate if the networked management interfaces are accessible from the public internet, and apply newly released updates from F5. .

Threat actors and malware

TikTok videos continue to push infostealers in ClickFix attacks

BleepingComputer - 19 October 2025 15:28

Cybercriminals are using TikTok videos disguised as free activation guides for popular software like Windows, Spotify, and Netflix to spread information-stealing malware. [...]

Over 266,000 F5 BIG-IP instances exposed to remote attacks

BleepingComputer - 17 October 2025 09:16

Internet security nonprofit Shadowserver Foundation has found more than 266,000 F5 BIG-IP instances exposed online after the security breach disclosed by cybersecurity company F5 this week. [...]

Microsoft Disrupts Ransomware Campaign Abusing Azure Certificates

darkreading - 17 October 2025 19:00

Microsoft revoked more than 200 digital certificates that threat actors used to sign fake Teams binaries that set the stage for Rhysida ransomware attacks.

China Accuses US of Cyberattack on National Time Center

SecurityWeek - 20 October 2025 01:58

The Ministry of State Security alleged that the NSA exploited vulnerabilities in the messaging services of a foreign mobile phone brand to steal sensitive information.

UK related

From Airport chaos to cyber intrigue: Everest Gang takes credit for Collins Aerospace breach

Security Affairs - 18 October 2025 16:10

Everest claims Collins Aerospace hack hitting EU airports, but its leak site vanishes soon after, sparking takedown speculation. Do you remember the Collins Aerospace supply chain attack that disrupted operations at several major European airports, including Heathrow in London, Brussels, and Berlin?