Scottish Cyber Coordination Centre

Daily Threat Bulletin

17 October 2025

Vulnerabilities

Gladinet fixes actively exploited zero-day in file-sharing software

BleepingComputer - 16 October 2025 12:11

Gladinet has released security updates for its CentreStack business solution to address a local file inclusion vulnerability (CVE-2025-11371) that threat actors have leveraged as a zero-day.

Operation Zero Disco: Threat actors targets Cisco SNMP flaw to drop Linux rootkits

Security Affairs - 16 October 2025 20:52

Trend Micro researchers disclosed details of a new campaign, tracked as Operation Zero Disco, that exploited a recently disclosed security flaw impacting Cisco IOS Software and IOS XE Software to deploy Linux rootkits on older, unprotected systems.

Fuji Electric HMI Configurator Flaws Expose Industrial Organizations to Hacking

SecurityWeek - 16 October 2025 12:57

Fuji Electric has released patches and Japan's JPCERT has informed organizations about the vulnerabilities.

Threat actors and malware

F5 Hack: Attack Linked to China, BIG-IP Flaws Patched, Governments Issue Alerts

SecurityWeek - 16 October 2025 09:41

More information has come to light on the cyberattack disclosed this week by F5, including on attribution and potential risks.

China-linked APT Jewelbug targets Russian IT provider in rare cross-nation cyberattack

Security Affairs - 16 October 2025 15:08

China-linked APT Jewelbug targeted a Russian IT provider for five months in 2025, showing Russia remains exposed to Chinese cyber espionage.

Microsoft Revokes Over 200 Certificates to Disrupt Ransomware Campaign

SecurityWeek - 16 October 2025 15:42

Microsoft announced on Wednesday that it has disrupted a Vanilla Tempest campaign whose goal was the deployment of Rhysida ransomware.