

Daily Threat Bulletin

9 October 2026

Vulnerabilities

Cisco warns of critical flaws allowing Nexus switch takeover

BleepingComputer - 08 October 2026 12:26

Cisco released security advisories for five critical vulnerabilities in its NX-OS data center network operating system that could be exploited to run arbitrary code with root privileges on Nexus switches.

Atlassian Vulnerability Comes Under Attack Hours After Details Go Public

Security Affairs - 08 October 2026 08:26

Threat actors are exploiting CVE-2026-21589, a critical Atlassian flaw that can expose sensitive files across multiple Data Center products. Threat actors have started exploiting CVE-2026-21589 (CVSS score of 9.3), a critical arbitrary file access flaw in Atlassian Data Center products.

SonicWall and Splunk Patch Critical Vulnerabilities

SecurityWeek - 08 October 2026 13:37

Critical and high-severity vulnerabilities could allow attackers to bypass authentication, execute arbitrary code, and elevate their privileges.

TP-Link Faces State Lawsuits and New Scrutiny Over ISP Router Flaws

SecurityWeek - 08 October 2026 11:24

SEC Consult has published technical details on vulnerabilities mentioned in a complaint filed by several US states.

Threat actors and malware

FakeGit malware campaign returns with 17,610 malicious GitHub repos

BleepingComputer - 08 October 2026 14:10

More than 17,000 fake repositories on GitHub are distributing the SmartLoader malware after the FakeGit campaign reactivated earlier this month to push the StealC infostealer.

ASOS links data breach to social engineering attack, credential theft

BleepingComputer - 08 October 2026 08:42

ASOS is sending updates to affected customers about the cybersecurity incident it suffered earlier this week, confirming that hackers accessed some personal data.



Scottish
Cyber
Coordination
Centre

Italy's Foreign Ministry Under Cyberattack as Embassy Sites Come Under Review

Security Affairs - 08 October 2026 20:33

Italy's Foreign Ministry is defending its website against a cyberattack, checking embassy sites and pushing for EU action to identify attackers. On the morning of October 8, Italy's Ministry of Foreign Affairs said its website was being attacked.

UAC-0099 Targets Ukrainian Government Personnel With ASHVEIN RAT Hiding Commands in HTML

The Hacker News - 08 October 2026 21:56

The Russia-aligned threat actor known as UAC-0099 has been attributed to a previously undocumented .NET infostealer and remote access trojan (RAT) codenamed ASHVEIN. According to TrendAI, the malware has been put to use in attacks targeting Ukrainian government personnel.

Russia-Aligned UAC-0099 Evolves MATCHBOIL Malware

Infosecurity Magazine - 08 October 2026 14:00

Russia-aligned UAC-0099 has steadily upgraded its MATCHBOIL downloader since 2024.

FBI disrupts Chinese hacking tools used to breach critical infrastructure

BleepingComputer - 08 October 2026 18:42

The FBI has seized seven domains used by Chinese state-sponsored hackers known as Flax Typhoon to operate two hacking tools, MicroScan and FishHub, used in attacks that breached critical infrastructure and other organizations worldwide.