Scottish Cyber Coordination Centre

Daily Threat Bulletin

29 July 2025

Vulnerabilities

Exploit available for critical Cisco ISE bug exploited in attacks

BleepingComputer - 28 July 2025 14:29

Security researcher Bobby Gould has published a blog post demonstrating a complete exploit chain for CVE-2025-20281, an unauthenticated remote code execution vulnerability in Cisco Identity Services Engine (ISE). [...]

Microsoft uncovers macOS flaw allowing bypass TCC protections and exposing sensitive data

Security Affairs - 29 July 2025 01:01

Microsoft found a macOS flaw letting attackers access private data from protected areas like Downloads and Apple Intelligence caches.

Critical Flaws in WordPress Plugin Leave 10,000 Sites Vulnerable

Infosecurity Magazine - 28 July 2025 16:05

10,000 WordPress sites vulnerable to takeover due to critical flaws in HT Contact Form Widget plugin

CISA Adds Three Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added three new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.CVE-2025-20281 Cisco Identity Services Engine Injection Vulnerability: CVE-2025-20337 Cisco Identity Services Engine Injection Vulnerability, CVE-2023-2533 PaperCut NG/MF Cross-Site Request Forgery (CSRF) Vulnerability.

Threat actors and malware

Scattered Spider targets VMware ESXi in using social engineering

Security Affairs - 28 July 2025 11:40

Scattered Spider targets VMware ESXi in North America using social engineering, mainly fake IT help desk calls instead of software exploits. The cybercrime group Scattered Spider (aka 0ktapus, Muddled Libra, Octo Tempest, and UNC3944) is targeting VMware ESXi hypervisors in retail, airline, and transportation sectors across North America.

China-linked group Fire Ant exploits VMware and F5 flaws since early 2025

Scottish Cyber Coordination Centre

Security Affairs - 28 July 2025 09:26

China-linked group Fire Ant exploits VMware and F5 flaws to stealthily breach secure systems, reports cybersecurity firm Sygnia. China-linked cyberespionage group Fire Ant is exploiting VMware and F5 vulnerabilities to stealthily access secure, segmented systems, according to Sygnia.

Hackers Breach Toptal GitHub, Publish 10 Malicious npm Packages With 5,000 Downloads

The Hacker News - 29 July 2025 00:01

In what's the latest instance of a software supply chain attack, unknown threat actors managed to compromise Toptal's GitHub organization account and leveraged that access to publish 10 malicious packages to the npm registry.

Chaos Ransomware Rises as BlackSuit Gang Falls

darkreading - 28 July 2025 20:20

Researchers detailed a newer double-extortion ransomware group made up of former members of BlackSuit, which was recently disrupted by international law enforcement.

Sophisticated Shuyal Stealer Targets 19 Browsers, Demonstrates Advanced Evasion

darkreading - 28 July 2025 16:30

A new infostealing malware making the rounds can exfiltrate credentials and other system data even from browsing software considered more privacy-focused than mainstream options.

Social engineering attack obtains data on 'majority' of Allianz Life customers

The Record from Recorded Future News - 28 July 2025 12:50