Daily Threat Bulletin

27 June 2025

Vulnerabilities

Cisco warns of max severity RCE flaws in Identity Services Engine

BleepingComputer - 26 June 2025 12:20

Cisco has published a bulletin to warn about two critical, unauthenticated remote code execution (RCE) vulnerabilities affecting Cisco Identity Services Engine (ISE) and the Passive Identity Connector (ISE-PIC).

CISA Warns AMI BMC Vulnerability Exploited in the Wild

SecurityWeek - 26 June 2025 11:06

CISA is urging federal agencies to patch a recent AMI BMC vulnerability and a half-a-decade-old bug in FortiOS by July 17.

Threat actors and malware

Microsoft 365 'Direct Send' abused to send phishing as internal users

BleepingComputer - 26 June 2025 10:00

An ongoing phishing campaign abuses a little-known feature in Microsoft 365 called "Direct Send" to evade detection by email security and steal credentials.

New FileFix Method Emerges as a Threat Following 517% Rise in ClickFix Attacks

The Hacker News - 26 June 2025 19:33

The ClickFix social engineering tactic as an initial access vector using fake CAPTCHA verifications increased by 517% between the second half of 2024 and the first half of this year, according to data from ESET.

3 key takeaways from the Scattered Spider attacks on insurance firms

BleepingComputer - 26 June 2025 11:02

Scattered Spider recently pivoted from targeting worldwide retailers to U.S. based insurance firms, with no signs of slowing down.

Kai West, aka IntelBroker, indicted for cyberattacks causing $25M in damages

Security Affairs - 26 June 2025 19:21

British national Kai West, aka IntelBroker, was charged in U.S. for a global hacking scheme that stole and sold data, causing millions in damages.