

Daily Threat Bulletin

15 January 2026

Vulnerabilities

[Fortinet fixed two critical flaws in FortiFone and FortiSIEM](#)

Security Affairs - 14 January 2026 16:07

Fortinet released patches for six vulnerabilities, including two critical flaws in FortiFone and FortiSIEM that could be exploited without authentication to leak configuration data or enable code execution.

[Critical Node.js Vulnerability Can Cause Server Crashes via async_hooks Stack Overflow](#)

The Hacker News - 14 January 2026 13:35

Node.js has released updates to fix what it described as a critical security issue impacting “virtually every production Node.js app” that, if successfully exploited, could trigger a denial-of-service (DoS) condition.

[Chrome 144, Firefox 147 Patch High-Severity Vulnerabilities](#)

SecurityWeek - 14 January 2026 10:50

The two browser updates resolve 26 security defects, including bugs that could be exploited for code execution.

[Microsoft Patch Tuesday security updates for January 2026 fixed actively exploited zero-day](#)

Security Affairs - 14 January 2026 09:43

Microsoft Patch Tuesday security updates for January 2026 release 112 CVEs affecting Windows, Office, Azure, Edge, SharePoint, SQL Server, SMB, and Windows management services.

Threat actors and malware

[Hackers Exploit c-ares DLL Side-Loading to Bypass Security and Deploy Malware](#)

The Hacker News - 14 January 2026 20:48

Security experts have disclosed details of an active malware campaign that’s exploiting a DLL side-loading vulnerability in a legitimate binary associated with the open-source c-ares library to bypass security controls and deliver a wide range of commodity trojans and stealers.



Scottish
Cyber
Coordination
Centre

ConsentFix debrief: Insights from the new OAuth phishing attack

BleepingComputer - 14 January 2026 11:01

ConsentFix is an OAuth phishing technique abusing browser-based authorization flows to hijack Microsoft accounts. Push Security shares new insights from continued tracking, community research, and evolving attacker techniques.

Predator Spyware Turns Failed Attacks Into Intelligence for Future Exploits

SecurityWeek - 14 January 2026 15:00

The Predator spyware is more sophisticated and dangerous than previously realized.

'VoidLink' Malware Poses Advanced Threat to Linux Systems

darkreading - 14 January 2026 16:59

Researchers discovered a modular, "cloud-first" framework that is feature-rich and designed to maintain stealthy, long-term access to Linux environments.

Criminal Subscription Service Behind AI-Powered Cyber-Attacks Taken Out By Microsoft

Infosecurity Magazine - 14 January 2026 17:32

RedVDS cyber-crime-as-a-service platform powering phishing, BEC attacks and other fraud has cost victims millions

UK incidents

UK backtracks on digital ID requirement for right to work

The Register - 14 January 2026 13:20

The UK government has backed down from making digital ID mandatory for proof of a right to work in the country, adding to confusion over the scheme's cost and purpose.