Scottish Cyber Coordination Centre

Daily Threat Bulletin

20 January 2026

Vulnerabilities

Google Gemini Prompt Injection Flaw Exposed Private Calendar Data via Malicious Invites

The Hacker News - 19 January 2026 23:51

Cybersecurity researchers have disclosed details of a security flaw that leverages indirect prompt injection targeting Google Gemini as a way to bypass authorization guardrails and use Google Calendar as a data extraction mechanism.

New StackWarp Hardware Flaw Breaks AMD SEV-SNP Protections on Zen 1–5 CPUs

The Hacker News - 19 January 2026 18:01

A team of academics from the CISPA Helmholtz Center for Information Security in Germany has disclosed the details of a new hardware vulnerability affecting AMD processors.

Security Bug in StealC Malware Panel Let Researchers Spy on Threat Actor Operations

The Hacker News - 19 January 2026 13:23

Cybersecurity researchers have disclosed a cross-site scripting (XSS) vulnerability in the web-based control panel used by operators of the StealC information stealer, allowing them to gather crucial insights on one of the threat actors using the malware in their operations.

Windows 11 shutdown bug forces Microsoft into out-of-band damage control

The Register - 19 January 2026 14:05

Ships emergency update to fix a Patch Tuesday misfire that prevented systems from switching off Microsoft has rushed out an out-of-band Windows 11 update after January's Patch Tuesday broke something as fundamental as turning PCs off.

TP-Link Patches Vulnerability Exposing VIGI Cameras to Remote Hacking

SecurityWeek - 19 January 2026 15:39

The researcher who discovered the vulnerability saw more than 2,500 internet-exposed devices.

Threat actors and malware

Fake ad blocker extension crashes the browser for ClickFix attacks

BleepingComputer - 19 January 2026 18:49

A malvertising campaign is using a fake ad-blocking Chrome and Edge extension named NexShield that intentionally crashes the browser in preparation for ClickFix attacks. [...]

New PDFSider Windows malware deployed on Fortune 100 firm's network

BleepingComputer - 19 January 2026 17:00

Ransomware attackers targeting a Fortune 100 company in the finance sector used a new malware strain, dubbed PDFSider, to deliver malicious payloads on Windows systems. [...]

Ransomware attack on Ingram Micro impacts 42,000 individuals

Security Affairs - 19 January 2026 19:29

Ingram Micro says a ransomware attack exposed personal data of about 42,000 people, including names, birth dates, SSNs, and job-related details. Ingram Micro is a global technology distributor and supply-chain services company. It acts as a middleman between IT vendors (like Microsoft, Cisco, HP, Apple, and cybersecurity firms) and businesses, resellers, and service providers, helping [...]

Hacker pleads guilty to hacking Supreme Court, AmeriCorps, and VA Systems

Security Affairs - 19 January 2026 09:15

An actor who goes online with the alias @ihackthegovernment posted stolen personal data from his victims, including the U.S. Supreme Court. Nicholas Moore, 24, from Tennessee, pleaded guilty to repeatedly hacking the U.S. Supreme Court's electronic filing system.

UK related

UK govt. warns about ongoing Russian hacktivist group attacks

BleepingComputer - 19 January 2026 13:20

The U.K. government is warning of continued malicious activity from Russian-aligned hacktivist groups targeting critical infrastructure and local government organizations in the country in disruptive denial-of-service (DDoS) attacks. [...]