Scottish Cyber Coordination Centre

Daily Threat Bulletin

17 February 2026

Vulnerabilities

CISA gives feds 3 days to patch actively exploited BeyondTrust flaw

BleepingComputer - 16 February 2026 08:33

CISA ordered U.S. government agencies on Friday to secure their BeyondTrust Remote Support instances against an actively exploited vulnerability within three days. [...]

Google fixes first actively exploited Chrome zero-day of 2026

Security Affairs - 16 February 2026 11:10

Google patched Chrome zero-day CVE-2026-2441, a high-severity CSS use-after-free flaw actively exploited in the wild. Google has released urgent security updates to address a high-severity zero-day vulnerability, tracked as CVE-2026-2441, in Chrome that is already being exploited in real-world attacks.

Vulnerabilities in Password Managers Allow Hackers to View and Change Passwords

Infosecurity Magazine - 16 February 2026 18:15

Security researchers have challenged end-to-end encryption claims from popular commercial password managers

Threat actors and malware

Infostealer malware found stealing OpenClaw secrets for first time

BleepingComputer - 16 February 2026 13:32

With the massive adoption of the OpenClaw agentic AI assistant, information-stealing malware has been spotted stealing files associated with the framework that contain API keys, authentication tokens, and other secrets. [...]

Microsoft alerts on DNS-based ClickFix variant delivering malware via nslookup

Security Affairs - 16 February 2026 13:24

Microsoft warns of a new ClickFix variant that tricks users into running DNS commands to fetch malware via nslookup. Microsoft has revealed a new ClickFix variant that deceives users into running a malicious nslookup command through the Windows Run dialog to retrieve a second-stage payload via DNS. ClickFix typically uses fake CAPTCHA or error messages [...]