Scottish Cyber Coordination Centre

Daily Threat Bulletin

20 February 2026

Vulnerabilities

Flaw in Grandstream VoIP phones allows stealthy eavesdropping

BleepingComputer - 19 February 2026 13:16

A critical vulnerability in Grandstream GXP1600 series VoIP phones allows a remote, unauthenticated attacker to gain root privileges and silently eavesdrop on communications. [...]

CISA orders feds to patch actively exploited Dell flaw within 3 days

BleepingComputer - 19 February 2026 11:30

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) ordered government agencies to patch their systems within three days against a maximum-severity Dell vulnerability that has been under active exploitation since mid-2024. [...]

U.S. CISA adds Dell RecoverPoint and GitLab flaws to its Known Exploited Vulnerabilities catalog

Security Affairs - 19 February 2026 16:16

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds Dell RecoverPoint and GitLab flaws to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added Dell RecoverPoint and GitLab flaws to its Known Exploited Vulnerabilities (KEV) catalog.

Ivanti Exploitation Surges as Zero-Day Attacks Traced Back to July 2025

SecurityWeek - 19 February 2026 12:56

Security researchers have seen the vulnerabilities being exploited to deliver shells, conduct reconnaissance, and download malware.

Industrial Control System Vulnerabilities Hit Record Highs

Infosecurity Magazine - 19 February 2026 14:00

Forescout paper reveals ICS advisories hit a record 508 in 2025

Flaws in Popular Software Development App Extensions Allow Data Exfiltration

Infosecurity Magazine - 19 February 2026 11:45

Four serious new vulnerabilities affect Microsoft Visual Studio Code, Cursor and Windsurf extensions, three of which remain unpatched

Scottish Cyber Coordination Centre

Researchers Reveal Six New OpenClaw Vulnerabilities

Infosecurity Magazine - 19 February 2026 11:00

Endor Labs has published details of six new vulnerabilities in popular AI assistant OpenClaw

Threat actors and malware

Hackers target Microsoft Entra accounts in device code vishing attacks

BleepingComputer - 19 February 2026 08:30

Threat actors are targeting technology, manufacturing, and financial organizations in campaigns that combine device code phishing and voice phishing (vishing) to abuse the OAuth 2.0 Device Authorization flow and compromise Microsoft Entra accounts. [...]

PromptSpy Android Malware Abuses Gemini AI to Automate Recent-Apps Persistence

The Hacker News - 20 February 2026 00:22

Cybersecurity researchers have discovered what they say is the first Android malware that abuses Gemini, Google's generative artificial intelligence (AI) chatbot, as part of its execution flow and achieves persistence.The malware has been codenamed PromptSpy by ESET.

Fake IPTV Apps Spread Massiv Android Malware Targeting Mobile Banking Users

The Hacker News - 19 February 2026 16:54

Cybersecurity researchers have disclosed details of a new Android trojan called Massiv that's designed to facilitate device takeover (DTO) attacks for financial theft.