Scottish
Cyber
Coordination
Centre

# Daily Threat Bulletin

23 February 2026

## Vulnerabilities

### CISA: BeyondTrust RCE flaw now exploited in ransomware attacks

BleepingComputer - 20 February 2026 13:02

Hackers are actively exploiting the CVE-2026-1731 vulnerability in the BeyondTrust Remote Support product, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) warns. [...]

### Anthropic unveils Claude Code Security to detect and fix code bugs

Security Affairs - 23 February 2026 01:11

Anthropic launches Claude Code Security, an AI tool that scans code for vulnerabilities and suggests how to address them. Anthropic has introduced Claude Code Security, a new AI-powered service designed to scan software codebases for vulnerabilities and recommend fixes. Built into Claude Code, the tool aims to help teams detect and remediate security flaws faster. [...]

### U.S. CISA adds RoundCube Webmail flaws to its Known Exploited Vulnerabilities catalog

Security Affairs - 21 February 2026 12:19

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds RoundCube Webmail flaws to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added two RoundCube Webmail flaws to its Known Exploited Vulnerabilities (KEV) catalog. Below are the flaws added to the catalog: Roundcube is a popular webmail platform and has been repeatedly targeted [...]

### CISA gives federal agencies three days to patch actively exploited Dell bug

The Register - 20 February 2026 13:13

Hardcoded credential flaw in RecoverPoint already abused in espionage campaign Uncle Sam's cyber defenders have given federal agencies just three days to patch a maximum-severity Dell bug that's been under active exploitation since at least mid-2024....

### Critical Grandstream Phone Vulnerability Exposes Calls to Interception

SecurityWeek - 21 February 2026 13:00

The flaw tracked as CVE-2026-2329 can be exploited without authentication for remote code execution with root privileges.

## Threat actors and malware

Scottish Cyber Coordination Centre

### Amazon: AI-assisted hacker breached 600 Fortinet firewalls in 5 weeks

BleepingComputer - 21 February 2026 09:50

Amazon is warning that a Russian-speaking hacker used multiple generative AI services as part of a campaign that breached more than 600 FortiGate firewalls across 55 countries in five weeks. [...]

### Cline CLI 2.3.0 Supply Chain Attack Installed OpenClaw on Developer Systems

The Hacker News - 20 February 2026 20:50

In yet another software supply chain attack, the open-source, artificial intelligence (AI)-powered coding assistant Cline CLI was updated to stealthily install OpenClaw, a self-hosted autonomous AI agent that has become exceedingly popular in the past few months."On February 17, 2026, at 3:26 AM PT, an unauthorized party used a compromised npm publish token to publish an update to Cline CLI

### ClickFix Campaign Abuses Compromised Sites to Deploy MIMICRAT Malware

The Hacker News - 20 February 2026 18:25

Cybersecurity researchers have disclosed details of a new ClickFix campaign that abuses compromised legitimate sites to deliver a previously undocumented remote access trojan (RAT) called MIMICRAT (aka AstarionRAT)."The campaign demonstrates a high level of operational sophistication: compromised sites spanning multiple industries and geographies serve as delivery infrastructure, a multi-stage

### PromptSpy Android Malware Abuses Gemini AI at Runtime for Persistence

SecurityWeek - 20 February 2026 08:06

The malware leverages Gemini to analyze on-screen elements and ensure that it remains on the device even after a reboot.

### Dramatic Escalation in Frequency and Power of DDoS Attacks

Infosecurity Magazine - 20 February 2026 13:30

DDoS attack frequency has risen to 'alarming levels,' warns Radware report