Scottish Cyber Coordination Centre

Daily Threat Bulletin

16 March 2026

Vulnerabilities

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation: CVE-2026-3909 Google Skia Out-of-Bounds Write Vulnerability; CVE-2026-3910 Google Chromium V8 Unspecified Vulnerability.

Microsoft releases Windows 11 OOB hotpatch to fix RRAS RCE flaw

BleepingComputer - 14 March 2026 18:48

Microsoft has released an out-of-band (OOB) update to fix a security vulnerabilities affecting Windows 11 Enterprise devices that receive hotpatch updates instead of the regular Patch Tuesday cumulative updates. [...]

OpenClaw AI Agent Flaws Could Enable Prompt Injection and Data Exfiltration

The Hacker News - 14 March 2026 22:47

China's National Computer Network Emergency Response Technical Team (CNCERT) has issued a warning about the security stemming from the use of OpenClaw (formerly Clawdbot and Moltbot), an open-source and self-hosted autonomous artificial intelligence (AI) agent.In a post shared on WeChat, CNCERT noted that the platform's "inherently weak default security configurations,"

Nine CrackArmor Flaws in Linux AppArmor Enable Root Escalation, Bypass Container Isolation

The Hacker News - 13 March 2026 14:48

Cybersecurity researchers have disclosed multiple security vulnerabilities within the Linux kernel's AppArmor module that could be exploited by unprivileged users to circumvent kernel protections, escalate to root, and undermine container isolation guarantees.

Veeam Patches 7 Critical Backup & Replication Flaws Allowing Remote Code Execution

The Hacker News - 13 March 2026 10:45

Veeam has released security updates to address multiple critical vulnerabilities in its Backup & Replication software that, if successfully exploited, could result in remote code execution.The vulnerabilities are as follows -CVE-2026-21666 (CVSS score: 9.9) - A vulnerability that allows an authenticated domain user to perform remote code execution on the Backup Server.CVE-2026-21667 (

Scottish Cyber Coordination Centre

Threat actors and malware

AI-assisted Slopoly malware powers Hive0163's ransomware campaigns

Security Affairs - 13 March 2026 12:36

The Hive0163 group used AI-assisted malware called Slopoly to maintain persistent access in ransomware attacks. IBM X-Force researchers report that the financially motivated group Hive0163 is using AI-assisted malware named Slopoly to maintain persistent access during ransomware attacks, showing how threat actors can quickly build new malware frameworks using AI.

Android 17 Blocks Non-Accessibility Apps from Accessibility API to Prevent Malware Abuse

The Hacker News - 16 March 2026 12:13

Google is testing a new security feature as part of Android Advanced Protection Mode (AAPM) that prevents certain kinds of apps from using the accessibility services API.The change, incorporated in Android 17 Beta 2, was first reported by Android Authority last week.

GlassWorm Supply-Chain Attack Abuses 72 Open VSX Extensions to Target Developers

The Hacker News - 14 March 2026 19:25

Cybersecurity researchers have flagged a new iteration of the GlassWorm campaign that they say represents a "significant escalation" in how it propagates through the Open VSX registry.

Most Google Cloud Attacks Start With Bug Exploitation

darkreading - 13 March 2026 14:20

Forget stolen credentials and misconfigurations; AI means vulnerability exploits that beat patching cycles are the top cause of compromises in the cloud.

UK related

Lloyds Banking Group Investigates Mobile App Data Exposure Affecting Multiple UK Banks

Security Boulevard - 15 March 2026 16:00

Lloyds Banking Group has launched an internal investigation after a technical error in its mobile banking applications allowed some customers to briefly see other users' transaction details. The incident affected the mobile apps of several brands operated by the group, including Lloyds Bank, Halifax, and Bank of Scotland.