Scottish Cyber Coordination Centre

Daily Threat Bulletin

05 March 2025

Vulnerabilities

Cisco warns of Webex for BroadWorks flaw exposing credentials

BleepingComputer - 04 March 2025 14:40

Cisco warned customers today of a vulnerability in Webex for BroadWorks that could let unauthenticated attackers access credentials remotely.

Google fixes Android zero-day exploited by Serbian authorities

BleepingComputer - 04 March 2025 07:38

Google has released patches for 43 vulnerabilities in Android's March 2025 security update, including two zero-days. Serbian authorities have used one of the zero-days to unlock confiscated devices.

VMware fixed three actively exploited zero-days in ESX products

Security Affairs - 05 March 2025 00:39

Broadcom released security updates to address three VMware zero-day vulnerabilities in ESX products that are actively exploited in the wild. The flaws, respectively tracked as CVE-2025-22224, CVE-2025-22225, and CVE-2025-22226, impact multiple VMware ESX products, including VMware ESXi, vSphere, Workstation, Fusion, Cloud Foundation, and Telco Cloud Platform.

CISA Adds Four Known Exploited Vulnerabilities to Catalog

CISA Advisories - 04 March 2025

CISA has added four new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation.

CVE-2024-50302 Linux Kernel Use of Uninitialized Resource Vulnerability.

CVE-2025-22225 VMware ESXi Arbitrary Write Vulnerability.

CVE-2025-22224 VMware ESXi and Workstation TOCTOU Race Condition Vulnerability.

CVE-2025-22226 VMware ESXi, Workstation, and Fusion Information Disclosure Vulnerability

Vulnerabilities Patched in Qualcomm, Mediatek Chipsets

SecurityWeek - 04 March 2025 13:38

Chip makers Qualcomm and Mediatek have released patches for many vulnerabilities across their products.

Scottish Cyber Coordination Centre

Threat actors and malware

New Eleven11bot botnet infects 86,000 devices for DDoS attacks

BleepingComputer - 04 March 2025 16:10

A new botnet malware named 'Eleven11bot' has infected over 86,000 IoT devices, primarily security cameras and network video recorders (NVRs), to conduct DDoS attacks.

New polyglot malware hits aviation, satellite communication firms

BleepingComputer - 04 March 2025 12:17

A previously undocumented polyglot malware is being deployed in attacks against aviation, satellite communication, and critical transportation organizations in the United Arab Emirates.

Mass exploitation campaign hit 4,000+ ISP networks to deploy info stealers and crypto miners

Security Affairs - 04 March 2025 12:51

The Splunk Threat Research Team discovered a mass exploitation campaign from Eastern Europe targeting ISPs in China and the U.S. West Coast to deploy info stealers and crypto miners.

Researchers Link CACTUS Ransomware Tactics to Former Black Basta Affiliates

The Hacker News - 04 March 2025 22:51

Threat actors deploying the Black Basta and CACTUS ransomware families have been found to rely on the same BackConnect (BC) module for maintaining persistent control over infected hosts, a sign that affiliates previously associated with Black Basta may have transitioned to CACTUS.

Threat Actor 'JavaGhost' Targets AWS Environments in Phishing Scheme

darkreading - 04 March 2025 22:26

Palo Alto Networks' Unit 42 details how a threat actor is dodging detection with careful targeting and the use of Amazon's native email tools.