Scottish Cyber Coordination Centre

Daily Threat Bulletin

25 July 2025

Vulnerabilities

CISA Adds Four Known Exploited Vulnerabilities to Catalog

CISA Advisories -

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

CVE-2025-54309 CrushFTP Unprotected Alternate Channel Vulnerability.

CVE-2025-6558 Google Chromium ANGLE and GPU Improper Input Validation Vulnerability.
CVE-2025-2776 SysAid On-Prem Improper Restriction of XML External Entity Reference Vulnerability.

CVE-2025-2775 SysAid On-Prem Improper Restriction of XML External Entity Reference Vulnerability

SonicWall Patches Critical SMA 100 Vulnerability, Warns of Recent Malware Attack

SecurityWeek - 24 July 2025 11:18

SonicWall advises organizations to patch SMA 100 appliances and look for IoCs associated with Overstep malware attacks.

Mitel warns of critical MiVoice MX-ONE authentication bypass flaw

BleepingComputer - 24 July 2025 12:17

Mitel Networks has released security updates to patch a critical-severity authentication bypass vulnerability impacting its MiVoice MX-ONE enterprise communications platform.

Fire Ant Exploits VMware Flaws to Compromise ESXi Hosts and vCenter Environments

The Hacker News - 24 July 2025 23:35

Virtualization and networking infrastructure have been targeted by a threat actor codenamed Fire Ant as part of a prolonged cyber espionage campaign.The activity, observed this year, is primarily designed Now to infiltrate organizations' VMware ESXi and vCenter environments as well as network appliances.

Scottish Cyber Coordination Centre

Threat actors and malware

Microsoft says Warlock ransomware deployed in SharePoint attacks as governments scramble

The Record from Recorded Future News - 24 July 2025 16:59

Microsoft has revealed that one of the threat actors behind the active exploitation of SharePoint flaws is deploying Warlock ransomware on targeted systems.

CastleLoader Malware Infects 469 Devices Using Fake GitHub Repos and ClickFix Phishing

The Hacker News - 24 July 2025 21:43

Cybersecurity researchers have shed light on a new versatile malware loader called CastleLoader that has been put to use in campaigns distributing various information stealers and remote access trojans (RATs).

Coyote malware is first-ever malware abusing Windows UI Automation

Security Affairs - 24 July 2025 21:43

New Coyote malware uses Windows UI Automation to steal banking credentials, targeting users across 75 banks and crypto platforms.

BlackSuit ransomware extortion sites seized in Operation Checkmate

BleepingComputer - 24 July 2025 18:34

Law enforcement has seized the dark web extortion sites of the BlackSuit ransomware operation, which has targeted and breached the networks of hundreds of organizations worldwide over the past several years.