Scottish Cyber Coordination Centre

Daily Threat Bulletin

10 April 2025

Vulnerabilities

CISA Warns of CentreStack's Hard-Coded MachineKey Vulnerability Enabling RCE Attacks

The Hacker News - 09 April 2025 14:30

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Tuesday added a critical security flaw impacting Gladinet CentreStack to its Known Exploited Vulnerabilities (KEV) catalog, citing evidence of active exploitation in the wild.

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Advisories -

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

- CVE-2024-53197 Linux Kernel Out-of-Bounds Access Vulnerability
- CVE-2024-53150 Linux Kernel Out-of-Bounds Read Vulnerability

Critical Fortinet FortiSwitch flaw allows remote attackers to change admin passwords

Security Affairs - 09 April 2025 18:50

Fortinet has released security updates to address a critical vulnerability, tracked as CVE-2024-48887 (CVSS score 9.8), in its FortiSwitch devices. A remote attacker can exploit the vulnerability to change administrator passwords.

Hackers target SSRF bugs in EC2-hosted sites to steal AWS credentials

BleepingComputer - 09 April 2025 17:58

A targeted campaign exploited Server-Side Request Forgery (SSRF) vulnerabilities in websites hosted on AWS EC2 instances to extract EC2 Metadata, which could include Identity and Access Management (IAM) credentials from the IMDSv1 endpoint.

Vulnerabilities Patched by Ivanti, VMware, Zoom

SecurityWeek - 09 April 2025 11:50

Ivanti, VMware, and Zoom released fixes for dozens of vulnerabilities in their products on April 2025 Patch Tuesday.

Scottish Cyber Coordination Centre

ICS Patch Tuesday: Vulnerabilities Addressed by Rockwell, ABB, Siemens, Schneider

SecurityWeek - 09 April 2025 09:54

Industrial giants Siemens, Rockwell, Schneider and ABB have released their March 2025 Patch Tuesday ICS security advisories.

Threat actors and malware

Oracle Faces Mounting Criticism as It Notifies Customers of Hack

SecurityWeek - 09 April 2025 11:10

Oracle is sending out written notifications to customers over the recent hack after it initially appeared to completely deny a data breach.

PipeMagic Trojan Exploits Windows Zero-Day Vulnerability to Deploy Ransomware

The Hacker News - 09 April 2025 14:34

Microsoft has revealed that a now-patched security flaw impacting the Windows Common Log File System (CLFS) was exploited as a zero-day in ransomware attacks aimed at a small number of targets.

New TCESB Malware Found in Active Attacks Exploiting ESET Security Scanner

The Hacker News - 09 April 2025 18:08

A Chinese-affiliated threat actor known for its cyber-attacks in Asia has been observed exploiting a security flaw in security software from ESET to deliver a previously undocumented malware codenamed TCESB.

Police detains Smokeloader malware customers, seizes servers

BleepingComputer - 09 April 2025 10:33

In follow-up activity for Operation Endgame, law enforcement tracked down Smokeloader botnet's customers and detained at least five individuals.

Phishing kits now vet victims in real-time before stealing credentials

BleepingComputer - 09 April 2025 10:49

Phishing actors are employing a new evasion tactic called 'Precision-Validated Phishing' that only shows fake login forms when a user enters an email address that the threat actors specifically targeted.