Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

14 March 2025

Vulnerabilities

GitLab patches critical authentication bypass vulnerabilities

BleepingComputer - 13 March 2025 13:13

GitLab released security updates for Community Edition (CE) and Enterprise Edition (EE), fixing nine vulnerabilities, among which two critical severity ruby-saml library authentication bypass flaws.

Experts warn of a coordinated surge in the exploitation attempts of SSRF vulnerabilities

Security Affairs - 13 March 2025 15:22

Intelligence firm GreyNoise observed Grafana path traversal exploitation attempts before the Server-Side Request Forgery (SSRF) surge on March 9, suggesting the attackers may be leveraging Grafana as an initial entry point for deeper exploitation.

Cisco Patches 10 Vulnerabilities in IOS XR

SecurityWeek - 13 March 2025 17:01

Cisco has released patches for 10 vulnerabilities in IOS XR, including five denial-of-service (DoS) bugs.

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-2025-24201** Apple Multiple Products WebKit Out-of-Bounds Write Vulnerability
- **CVE-2025-21590** Juniper Junos OS Improper Isolation or Compartmentalization Vulnerability

Threat actors and malware

New SuperBlack ransomware exploits Fortinet auth bypass flaws

BleepingComputer - 13 March 2025 16:57

A new ransomware operator named ‘Mora_001’ is exploiting two Fortinet vulnerabilities to gain unauthorized access to firewall appliances and deploy a custom ransomware strain dubbed SuperBlack.

OBSCURE#BAT Malware Highlights Risks of API Hooking

darkreading - 13 March 2025 22:22

Researchers discovered an attack chain that uses several layers of obfuscated batch files and PowerShell scripts to deliver an advanced and persistent rootkit.

North Korea-linked APT group ScarCruft spotted using new Android spyware KoSpy

Security Affairs - 13 March 2025 17:17

North Korea-linked threat actor ScarCruft (aka APT37, Reaper, and Group123) is behind a previously undetected Android surveillance tool named KoSpy that was used to target Korean and English-speaking users.

Microsoft Warns of ClickFix Phishing Campaign Targeting Hospitality Sector via Fake Booking[.]com Emails

The Hacker News - 13 March 2025 21:56

Microsoft has shed light on an ongoing phishing campaign that targeted the hospitality sector by impersonating online travel agency Booking.com using an increasingly popular social engineering technique called ClickFix to deliver credential-stealing malware.