Scottish Cyber Coordination Centre

Daily Threat Bulletin

24 March 2025

Vulnerabilities

Ongoing Cyber Attacks Exploit Critical Vulnerabilities in Cisco Smart Licensing Utility

The Hacker News - 21 March 2025 11:39

Two now-patched security flaws impacting Cisco Smart Licensing Utility are seeing active exploitation attempts, according to SANS Internet Storm Center.The two critical-rated vulnerabilities in question are listed below - CVE-2024-20439 (CVSS score: 9.8)

CVE-2025-29927 – Understanding the Next.js Middleware Vulnerability

Security Boulevard - 24 March 2025 06:16

When security vulnerabilities appear in popular frameworks, they can affect thousands of websites overnight. That's exactly what's happening with a newly discovered vulnerability in Next.js – one of the most...The post CVE-2025-29927 – Understanding the Next.js Middleware Vulnerability appeared first on Strobes Security.

In Other News: Critical Chrome Bug, Capital One Hacker Resententencing, Story of Expat Flaw

SecurityWeek - 21 March 2025 16:43

Noteworthy stories that might have slipped under the radar: Capital One hacker's sentence reversed, Google patches critical Chrome vulnerability, the story of an Expat flaw.

Threat actors and malware

Oracle denies breach after hacker claims theft of 6 million data records

BleepingComputer - 21 March 2025 17:43

Oracle denies it was breached after a threat actor claimed to be selling 6 million data records allegedly stolen from the company's Oracle Cloud federated SSO login servers [...]

Microsoft Trusted Signing service abused to code-sign malware

BleepingComputer - 22 March 2025 11:30

Cybercriminals are abusing Microsoft's Trusted Signing platform to code-sign malware executables with short-lived three-day certificates. [...]

RansomHub affiliate uses custom backdoor Betruger

Security Affairs - 21 March 2025 12:25

Scottish Cyber Coordination Centre

Symantec researchers linked a custom backdoor, called Betruger, found in recent ransomware attacks to an affiliate of the RansomHub operation. Symantec's Threat Hunter team has identified a custom backdoor, named Betruger, linked to a RansomHub affiliate. Designed for ransomware attacks, Betruger combines multiple functions into a single tool to minimize detection.

Medusa Ransomware Uses Malicious Driver to Disable Anti-Malware with Stolen Certificates

The Hacker News - 21 March 2025 19:28

The threat actors behind the Medusa ransomware-as-a-service (RaaS) operation have been observed using a malicious driver dubbed ABYSSWORKER as part of a bring your own vulnerable driver (BYOVD) attack designed to disable anti-malware tools.

China-Linked APT Aquatic Panda: 10-Month Campaign, 7 Global Targets, 5 Malware Families

The Hacker News - 21 March 2025 17:31

The China-linked advanced persistent threat (APT) group known as Aquatic Panda has been linked to a "global espionage campaign" that took place in 2022 targeting seven organizations.