Scottish Cyber Coordination Centre

Daily threat bulletin

19 September 2024

Vulnerabilities

GitLab releases fix for critical SAML authentication bypass flaw

BleepingComputer - 18 September 2024 15:37

GitLab has released security updates to address a critical SAML authentication bypass vulnerability impacting self-managed installations of the GitLab Community Edition (CE) and Enterprise Edition (EE). [...]

Patch Issued for Critical VMware vCenter Flaw Allowing Remote Code Execution

The Hacker News - 18 September 2024 11:38

Broadcom on Tuesday released updates to address a critical security flaw impacting VMware vCenter Server that could pave the way for remote code execution. The vulnerability, tracked as CVE-2024-38812 (CVSS score: 9.8), has been described as a heap-overflow vulnerability in the DCE/RPC protocol.

CISA, FBI Urge Organizations to Eliminate XSS Vulnerabilities

SecurityWeek - 18 September 2024 12:36

CISA and the FBI have released an alert on XSS vulnerabilities, urging organizations to adopt a secure by design approach and eliminate them.

Chrome 129 Patches High-Severity Vulnerability in V8 Engine

SecurityWeek - 18 September 2024 12:13

Google has released Chrome 129 with patches for nine vulnerabilities, including a high-severity bug in the V8 engine.The post Chrome 129 Patches High-Severity Vulnerability in V8 Engine appeared first on SecurityWeek.

Threat actors and malware

Microsoft: Vanilla Tempest hackers hit healthcare with INC ransomware

BleepingComputer - 18 September 2024 16:02

Microsoft says a ransomware affiliate it tracks as Vanilla Tempest now targets U.S. healthcare organizations in INC ransomware attacks. [...]

Chinese botnet infects 260,000 SOHO routers, IP cameras with malware

BleepingComputer - 18 September 2024 13:00

The FBI and cybersecurity researchers have disrupted a massive Chinese botnet called “Raptor Train” that infected over 260,000 networking devices to target critical infrastructure in the US and in other countries. […]

Contractor Software Targeted via Microsoft SQL Server Loophole

darkreading - 18 September 2024 21:51

By accessing the MSSQL, threat actors gain admin-level access to the application, allowing them to automate their attacks.

Chinese spies spent months inside aerospace engineering firm’s network via legacy IT

The Register - 18 September 2024 18:00

Getting sloppy, Xi Exclusive Chinese state-sponsored spies have been spotted inside a global engineering firm’s network, having gained initial entry using an admin portal’s default credentials on an IBM AIX server.

Europol Taskforce Disrupts Global Criminal Network Through Supply Chain Attack

Infosecurity Magazine - 18 September 2024 11:15

The suspected creator of Ghost, an encrypted communication platform allegedly used by organized crime groups worldwide, has been arrested.

UK related

QR Phishing Scams Gain Motorized Momentum in UK

darkreading - 18 September 2024 21:44

Criminal actors are finding their niche in utilizing QR phishing codes, otherwise known as "quishing," to victimize unsuspecting tourists in Europe and beyond.