Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

25 March 2025

Vulnerabilities

Critical flaw in Next.js lets hackers bypass authorization

BleepingComputer - 24 March 2025 13:15

A critical severity vulnerability has been discovered in the Next.js open-source web development framework, potentially allowing attackers to bypass authorization checks. [...]

Critical Ingress NGINX Controller Vulnerability Allows RCE Without Authentication

The Hacker News - 25 March 2025 01:25

A set of five critical security shortcomings have been disclosed in the Ingress NGINX Controller for Kubernetes that could result in unauthenticated remote code execution, putting over 6,500 clusters at immediate risk by exposing the component to the public internet. The vulnerabilities (CVE-2025-24513, CVE-2025-24514, CVE-2025-1097, CVE-2025-1098, and CVE-2025-1974).

Critical 'IngressNightmare' Vulns Imperil Kubernetes Environments

darkreading - 24 March 2025 20:10

More than 40% of all Internet-facing container orchestration clusters are at risk.

NIST Still Struggling to Clear Vulnerability Submissions Backlog in NVD

SecurityWeek - 24 March 2025 17:15

The effects of the backlog are already being felt in vulnerability management circles where NVD data promises an enriched source of truth.

Threat actors and malware

New VanHelsing ransomware targets Windows, ARM, ESXi systems

BleepingComputer - 24 March 2025 16:43

A new multi-platform ransomware-as-a-service (RaaS) operation named VanHelsing has emerged, targeting Windows, Linux, BSD, ARM, and ESXi systems. [...]

Medusa ransomware uses malicious Windows driver ABYSSWORKER to disable security tools

Security Affairs - 24 March 2025 15:56

Medusa ransomware uses a malicious Windows driver ABYSSWORKER to disable security tools, making detection and mitigation more difficult. Elastic Security Labs tracked a financially driven MEDUSA ransomware campaign using a HEARTCRYPT-packed loader and a revoked certificate-signed driver, ABYSSWORKER, to disable EDR tools. The attackers used a 64-bit Windows PE driver named smuol.sys, disguised as a […]

FBI warns of malicious free online document converters spreading malware

Security Affairs - 24 March 2025 09:14

The FBI warns of a significant increase in scams involving free online document converters to infect users with malware. The FBI warns that threat actors use malicious online document converters to steal users' sensitive information and infect their systems with malware. "The FBI Denver Field Office is warning that agents are increasingly seeing a scam […]

The Rise of OAuth Attacks to Access Sensitive Systems | Grip

Security Boulevard - 24 March 2025 23:32

OAuth attacks are increasing, exploiting SaaS blind spots to gain covert access. Learn how these attacks work and why visibility is key to mitigating the risks.

Oracle Denies Cloud Breach After Hacker Offers to Sell Data

SecurityWeek - 24 March 2025 16:51

Oracle has denied that Cloud systems have been breached after a hacker claimed to have stolen millions of records.

Albabat Ransomware Expands Targets, Abuses GitHub

SecurityWeek - 24 March 2025 11:10

New versions of the Albabat ransomware target Windows, Linux, and macOS, and retrieve configuration files from GitHub.