Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

18 July 2025

Vulnerabilities

Cisco patches critical CVE-2025-20337 bug in Identity Services Engine with CVSS 10 Severity

Security Affairs - 17 July 2025 11:29

Cisco addressed a critical vulnerability, tracked as CVE-2025-20337 (CVSS score of 10), in Identity Services Engine (ISE) and Cisco Identity Services Engine Passive Identity Connector (ISE-PIC).

Citrix Bleed 2 exploited weeks before PoCs as Citrix denied attacks

BleepingComputer - 17 July 2025 20:37

A critical Citrix NetScaler vulnerability, tracked as CVE-2025-5777 and dubbed “CitrixBleed 2,” was actively exploited nearly two weeks before proof-of-concept (PoC) exploits were made public, despite Citrix stating that there was no evidence of attacks.

VMware fixes four ESXi zero-day bugs exploited at Pwn2Own Berlin

BleepingComputer - 17 July 2025 18:36

VMware fixed four vulnerabilities in VMware ESXi, Workstation, Fusion, and Tools that were exploited as zero-days during the Pwn2Own Berlin 2025 hacking contest in May 2025.

Oracle Patches 200 Vulnerabilities With July 2025 CPU

SecurityWeek - 17 July 2025 08:25

Oracle’s July 2025 Critical Patch Update contains 309 security patches that address approximately 200 unique CVEs.

Threat actors and malware

Hackers Use GitHub Repositories to Host Amadey Malware and Data Stealers, Bypassing Filters

The Hacker News - 18 July 2025 00:10

Threat actors are leveraging public GitHub repositories to host malicious payloads and distribute them via Amadey as part of a campaign observed in April 2025.

LameHug malware uses AI LLM to craft Windows data-theft commands in real-time

BleepingComputer - 17 July 2025 15:57

A novel malware family named LameHug is using a large language model (LLM) to generate commands to be executed on compromised Windows systems.

UNC6148 deploys Overstep malware on SonicWall devices, possibly for ransomware operations

Security Affairs - 17 July 2025 08:47

Google's Threat Intelligence Group warns that a threat actor tracked as UNC6148 has been targeting SonicWall SMA appliances with new malware dubbed Overstep.

Microsoft Exposes Scattered Spider's Latest Tactics

Infosecurity Magazine - 17 July 2025 11:15

Microsoft has reported Scattered Spider continues to evolve tactics to compromise both on-premises infrastructure and cloud environments

Hacktivism Increasingly Targeting Critical Infrastructure

Security Magazine - 17 July 2025 09:00

Research from Cyble indicates that hacktivists are expanding beyond website defacements and DDoS attacks (which are typically connected with ideologically driven cyberattacks) and increasingly targeting critical infrastructure.