Scottish Cyber Coordination Centre

Daily threat bulletin

4 October 2024

Vulnerabilities

Cisco Patches Critical Vulnerability in Data Center Management Product

SecurityWeek - 03 October 2024 13:33

A critical-severity vulnerability in Cisco NDFC could allow attackers to execute commands with elevated privileges.

Apple iOS 18.0.1 Patches Password Exposure and Audio Snippet Bugs

SecurityWeek - 04 October 2024 01:22

According to a barebones Apple advisory, the new iOS 18.0.1 fixes two bugs that expose passwords and audio snippets to malicious hackers.

Google Adds New Pixel Security Features to Block 2G Exploits and Baseband Attacks

The Hacker News - 03 October 2024 23:30

Google has revealed the various security guardrails that have been incorporated into its latest Pixel devices to counter the rising threat posed by baseband security attacks.

Recently patched CUPS flaw can be used to amplify DDoS attacks

BleepingComputer - 03 October 2024 19:33

A recently disclosed vulnerability in the Common Unix Printing System (CUPS) open-source printing system can be exploited by threat actors to launch distributed denial-of-service (DDoS) attacks with a 600x amplification factor.

Litespeed Cache Plugin Flaw Allows XSS Attack, Update Now

Infosecurity Magazine - 03 October 2024 17:30

The new LiteSpeed Cache flaw (CVE-2024-47374) allows unauthenticated code injection across more than six million active installations.

Jenkins Patches High-Impact Vulnerabilities in Server and Plugins

SecurityWeek - 03 October 2024 14:35

Jenkins has released patches for multiple high- and medium-severity vulnerabilities impacting the automation tool and several plugins.

Threat actors and malware

Scottish Cyber Coordination Centre

New Perfctl Malware Targets Linux Servers for Cryptocurrency Mining and Proxyjacking

The Hacker News - 03 October 2024 20:45

Misconfigured and vulnerable Linux servers are the target of an ongoing campaign that delivers a stealthy malware dubbed perfctl with the primary aim of running a cryptocurrency miner and proxyjacking software.

Emulating the Surging Hadooken Malware

Security Boulevard - 03 October 2024 20:16

AttackIQ has released a new attack graph that emulates the behaviors exhibited by the Hadooken malware during intrusions that abused misconfigurations and critical Remote Code Execution (RCE) vulnerabilities on public-facing Oracle Weblogic Servers.

Ransomware crew infects 100+ orgs monthly with new MedusaLocker variant

The Register - 03 October 2024 11:00

An extortionist armed with a new variant of MedusaLocker ransomware has infected more than 100 organizations a month since at least 2022, according to Cisco Talos, which recently discovered a “substantial” Windows credential data dump that sheds light on the criminal and their victims.

Microsoft and US Government Disrupt Russian Star Blizzard Operations

Infosecurity Magazine - 03 October 2024 17:00

Microsoft and the US government have collectively seized over 100 websites used by Russian nation-state actor Star Blizzard.

Cloudflare mitigated new record-breaking DDoS attack of 3.8 Tbps

Security Affairs - 03 October 2024 14:01

Cloudflare recently mitigated a new record-breaking DDoS attack, peaking at 3.8 Tbps and 2.14 billion packets per second (Pps). Cloudflare reported that starting from early September, it has mitigated over 100 hyper-volumetric L3/4 DDoS attacks, with many exceeding 2 billion Pps and 3 Tbps.