Scottish Cyber Coordination Centre

Daily Threat Bulletin

3 April 2025

Vulnerabilities

U.S. CISA adds Apache Tomcat flaw to its Known Exploited Vulnerabilities catalog

Security Affairs - 02 April 2025 14:47

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds Apache Tomcat flaw to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added an Apache Tomcat path equivalence vulnerability, tracked as CVE-2025-24813, to its Known Exploited Vulnerabilities (KEV) catalog.

Apple backported fixes for three actively exploited flaws to older devices

Security Affairs - 02 April 2025 09:52

Apple backports three critical vulnerabilities actively exploited in attacks against older iOS and macOS models. Apple has backported fixes for three actively exploited vulnerabilities to older devices and OS versions.

Google Fixed Cloud Run Vulnerability Allowing Unauthorized Image Access via IAM Misuse

The Hacker News - 02 April 2025 20:18

Cybersecurity researchers have disclosed details of a now-patched privilege escalation vulnerability in Google Cloud Platform (GCP) Cloud Run that could have allowed a malicious actor to access container images and even inject malicious code.

Vulnerabilities Expose Jan AI Systems to Remote Manipulation

SecurityWeek - 02 April 2025 17:10

Vulnerabilities in open source ChatGPT alternative Jan AI expose systems to remote, unauthenticated manipulation.

Google DeepMind Unveils Framework to Exploit AI's Cyber Weaknesses

SecurityWeek - 02 April 2025 14:43

DeepMind found that current AI frameworks are ad hoc, not systematic, and fail to provide defenders with useful insights.

ImageRunner Flaw Exposed Sensitive Information in Google Cloud

SecurityWeek - 02 April 2025 13:10

Google has patched a Cloud Run vulnerability dubbed ImageRunner that could have been exploited to gain access to sensitive data.

Scottish Cyber Coordination Centre

[R1] Nessus Agent Version 10.7.4 Fixes One Vulnerability

Tenable Product Security Advisories - 02 April 2025 16:12

[R1] Nessus Agent Version 10.7.4 Fixes One VulnerabilityArnie CabralWed, 04/02/2025 - 11:12 When installing Nessus Agent to a non-default location on a Windows host, Nessus Agent versions prior to 10.7.4 did not enforce secure permissions for sub-directories. This could allow for local privilege escalation if users had not secured the directories in the non-default installation location.

Verizon Call Filter API flaw exposed customers' incoming call history

BleepingComputer - 02 April 2025 16:47

A vulnerability in Verizon's Call Filter feature allowed customers to access the incoming call logs for another Verizon Wireless number through an unsecured API request. [...]

Threat actors and malware

Counterfeit Android devices found preloaded with Triada malware

BleepingComputer - 02 April 2025 10:57

A new version of the Triada trojan has been discovered preinstalled on thousands of new Android devices, allowing threat actors to steal data as soon as they are set up. [...]

Cisco warns of CSLU backdoor admin account used in attacks

BleepingComputer - 02 April 2025 10:19

Cisco warns admins to patch a critical Cisco Smart Licensing Utility (CSLU) vulnerability, which exposes a built-in backdoor admin account now used in attacks. [...]

Spike in Palo Alto Networks scanner activity suggests imminent cyber threats

Security Affairs - 02 April 2025 08:29

Hackers are scanning for vulnerabilities in Palo Alto Networks GlobalProtect portals, likely preparing for targeted attacks. Researchers at the threat intelligence firm GreyNoise warn of hackers that are scanning for vulnerabilities in Palo Alto Networks GlobalProtect portals, likely preparing for targeted attacks, warns threat intelligence firm GreyNoise.

Legacy Stripe API Exploited to Validate Stolen Payment Cards in Web Skimmer Campaign

The Hacker News - 03 April 2025 11:15

Threat hunters are warning of a sophisticated web skimmer campaign that leverages a legacy application programming interface (API) from payment processor Stripe to validate stolen payment information prior to exfiltration.

North Korea's IT Operatives Are Exploiting Remote Work Globally

SecurityWeek - 02 April 2025 14:23

Scottish Cyber Coordination Centre

The global rise of North Korean IT worker infiltration poses a serious cybersecurity risk—using fake identities, remote access, and extortion to compromise organizations.