Scottish Cyber Coordination Centre

Daily threat bulletin

18 September 2024

Vulnerabilities

Broadcom fixes critical RCE bug in VMware vCenter Server

BleepingComputer - 17 September 2024 16:57

Broadcom has fixed a critical VMware vCenter Server vulnerability that attackers can exploit to gain remote code execution on unpatched servers via a network packet. [...]

GitLab releases security updates to fix 17 vulnerabilities

Security Magazine - 17 September 2024 13:00

GitLab releases a security update for a critical flaw. Security leaders share advice on how organizations can secure against this vulnerability.

Zero-Click RCE Bug in macOS Calendar Exposes iCloud Data

darkreading - 17 September 2024 22:26

A researcher bypassed the Calendar sandbox, Gatekeeper, and TCC in a chain attack that allowed for wanton theft of iCloud photos.

Google Cloud Document AI flaw (still) allows data theft despite bounty payout

The Register - 17 September 2024 21:15

Chocolate Factory downgrades risk, citing the need for attacker access Overly permissive settings in Google Cloud's Document AI service could be abused by data thieves to break into Cloud Storage buckets and steal sensitive information....

CISA Adds Four Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added four new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. CVE-2014-0497 Adobe Flash Player Integer Underflow Vulnerability, CVE-2013-0643 Adobe Flash Player Incorrect Default Permissions Vulnerability, CVE-2013-0648 Adobe Flash Player Code Execution Vulnerability, CVE-2014-0502 Adobe Flash Player Double Free Vulnerability.

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. CVE-2024-43461 Microsoft Windows MSHTML Platform Spoofing Vulnerability, CVE-2024-6670 Progress WhatsUp Gold SQL Injection Vulnerability.

Scottish Cyber Coordination Centre

Threat actors and malware

Ransomware gangs now abuse Microsoft Azure tool for data theft

BleepingComputer - 17 September 2024 13:14

Ransomware gangs like BianLian and Rhysida increasingly use Microsoft's Azure Storage Explorer and AzCopy to steal data from breached networks and store it in Azure Blob storage. [...]

Binance Warns of Rising Clipper Malware Attacks Targeting Cryptocurrency Users

The Hacker News - 17 September 2024 13:48

Cryptocurrency exchange Binance is warning of an "ongoing" global threat that's targeting cryptocurrency users with clipper malware with the goal of facilitating financial fraud.

CVE backlog update: The NVD struggles as attackers change tactics

Security Intelligence - 17 September 2024 14:00

In February, the number of vulnerabilities processed and enriched by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) started to slow. By May, 93.4% of new vulnerabilities and 50.8% of known exploited vulnerabilities were still waiting on analysis, according to research from VulnCheck.

UK related

Over Half of Breached UK Firms Pay Ransom

Infosecurity Magazine - 17 September 2024 10:00

Cohesity claims ransomware attacks are on the rise in the UK, with 59% of breached firms paying their extortionists.