Scottish Cyber Coordination Centre

Daily threat bulletin

13 November 2024

Vulnerabilities

Microsoft Patch Tuesday security updates for November 2024 fix two actively exploited zero-days

Security Affairs - 13 November 2024 01:45

Microsoft Patch Tuesday security updates for November 2024 addressed 89 vulnerabilities, including two actively exploited zero-day flaws. Microsoft Patch Tuesday security updates for November 2024 fixed 89 vulnerabilities in Windows and Windows Components; Office and Office Components; Azure; .NET and Visual Studio; LightGBM; Exchange Server; SQL Server; TorchGeo; Hyper-V; and Windows VMSwitch.

Patch Tuesday: Critical Flaws in Adobe Commerce, Photoshop, InDesign, Illustrator

SecurityWeek - 12 November 2024 19:01

Adobe patches critical-severity bugs in multiple products, including the Adobe Commerce and Magento Open Source platforms.

New Citrix Zero-Day Vulnerability Allows Remote Code Execution

Infosecurity Magazine - 12 November 2024 15:00

watchTowr has found a flaw in Citrix's Session Recording Manager that can be exploited to enable unauthenticated RCE against Citrix Virtual Apps and Desktops

SAP Patches High-Severity Vulnerability in Web Dispatcher

SecurityWeek - 12 November 2024 14:15

SAP has released eight new security notes on November 2024 patch day, including one addressing a high-severity vulnerability in Web Dispatcher.

Windows 10 KB5046613 update released with fixes for printer bugs

BleepingComputer - 12 November 2024 15:37

Microsoft has released the KB5046613 cumulative update for Windows 10 22H2 and Windows 10 21H2, which includes ten changes and fixes, including the new Microsoft account manager on the Start menu and fixes for multi-function printer issues. [...]

CISA, FBI, NSA, and International Partners Release Joint Advisory on 2023 Top Routinely Exploited Vulnerabilities

CISA Advisories -

Today, the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), National Security Agency (NSA), and international partners released joint

Scottish Cyber Coordination Centre

Cybersecurity Advisory, 2023 Top Routinely Exploited Vulnerabilities.This advisory supplies details on the top Common Vulnerabilities and Exposures (CVEs) routinely exploited by malicious cyber actors and their associated Common Weakness Enumeration(s) (CWE) to help organizations better understand the impact of exploitation.

Threat actors and malware

North Korea Hackers Leverage Flutter to Deliver macOS Malware

Infosecurity Magazine - 12 November 2024 14:00

Jamf observed North Korean attackers embedding malware within Flutter applications to target macOS devices, potentially to test a new way of weaponizing malware.

Ymir ransomware, a new stealthy ransomware grow in the wild

Security Affairs - 12 November 2024 11:26

New Ymir ransomware was deployed in attacks shortly after systems were breached by RustyStealer malware, Kaspersky warns. Kaspersky researchers discovered a new ransomware family, called Ymir ransomware, which attackers deployed after breaching systems via PowerShell commands.

'GoIssue' Cybercrime Tool Targets GitHub Developers En Masse

darkreading - 12 November 2024 18:44

Marketed on a cybercriminal forum, the $700 tool harvests email addresses from public GitHub profiles, priming cyberattackers for further credential theft, malware delivery, OAuth subversion, supply chain attacks, and other corporate breaches.

Volt Typhoon rebuilds malware botnet following FBI disruption

BleepingComputer - 12 November 2024 11:49

The Chinese state-sponsored hacking group Volt Typhoon has begun to rebuild its "KV-Botnet" malware botnet after it was disrupted by law enforcement in January, according to researchers from SecurityScorecard. [...]