Scottish Cyber Coordination Centre

Daily threat bulletin

31 October 2024

Vulnerabilities

Google fixed a critical vulnerability in Chrome browser

Security Affairs - 30 October 2024 13:05

Google addressed a critical vulnerability in its Chrome browser, tracked as CVE-2024-10487, which was reported by Apple. Google has patched a critical Chrome vulnerability, tracked as CVE-2024-10487, reported by Apple Security Engineering and Architecture (SEAR) on October 23, 2024.

QNAP patches second zero-day exploited at Pwn2Own to get root

BleepingComputer - 30 October 2024 14:36

QNAP has fixed a second zero-day vulnerability exploited at the Pwn2Own Ireland 2024 hacking contest to gain a root shell and take over a TS-464 NAS device. [...]

LiteSpeed Cache Plugin Vulnerability Poses Admin Access Risk

Infosecurity Magazine - 30 October 2024 18:15

The LiteSpeed Cache vulnerability allows administrator-level access, risking security for over 6 million WordPress sites

Fortinet Updates Guidance and Indicators of Compromise following FortiManager Vulnerability Exploitation

CISA Advisories -

Fortinet has updated their security advisory addressing a critical FortiManager vulnerability (CVE-2024-47575) to include additional workarounds and indicators of compromise (IOCs). A remote, unauthenticated cyber threat actor could exploit this vulnerability to gain access to sensitive files or take control of an affected system.

[R1] Sensor Proxy Version 1.0.11 Fixes Multiple Vulnerabilities

Tenable Product Security Advisories - 30 October 2024 18:41

[R1] Sensor Proxy Version 1.0.11 Fixes Multiple VulnerabilitiesArnie CabralWed, 10/30/2024 - 13:41 Sensor Proxy leverages third-party software to help provide underlying functionality.

Threat actors and malware

New version of Android malware FakeCall redirects bank calls to scammers

Security Affairs - 31 October 2024 01:52

The latest FakeCall malware version for Android intercepts outgoing bank calls, redirecting them to attackers to steal sensitive info and bank funds. Zimperium researchers spotted a new version of the FakeCall malware for Android that hijacks outgoing victims' calls and redirects them to the attacker's phone number.

Recent Version of LightSpy iOS Malware Packs Destructive Capabilities

SecurityWeek - 30 October 2024 11:58

A newer version of the LightSpy malware for iOS includes over a dozen new plugins, many with destructive capabilities.

Hackers steal 15,000 cloud credentials from exposed Git config files

BleepingComputer - 30 October 2024 11:00

A global large-scale dubbed "EmeraldWhale" exploited misconfigured Git configuration files to steal over 15,000 cloud account credentials from thousands of private repositories. [...]

Russia-linked Midnight Blizzard APT targeted 100+ organizations with a spear-phishing campaign using RDP files

Security Affairs - 30 October 2024 20:20

Microsoft warns of a new phishing campaign by Russia-linked APT Midnight Blizzard targeting hundreds of organizations. Microsoft warns of a large-scale spear-phishing campaign by Russia-linked APT Midnight Blizzard (aka APT29, SVR group, BlueBravo, Cozy Bear, Nobelium, Midnight Blizzard, and The Dukes), targeting 1,000+ users across 100+ organizations for intelligence gathering.

North Korean govt hackers linked to Play ransomware attack

BleepingComputer - 30 October 2024 12:55

The North Korean state-sponsored hacking group tracked as 'Andariel' has been linked to the Play ransomware operation, using the RaaS to work behind the scenes and evade sanctions. [...]