Scottish Cyber Coordination Centre

Daily threat bulletin

20 November 2024

Vulnerabilities

Oracle warns of Agile PLM file disclosure flaw exploited in attacks

BleepingComputer - 19 November 2024 15:56

Oracle has fixed an unauthenticated file disclosure flaw in Oracle Agile Product Lifecycle Management (PLM) tracked as CVE-2024-21287, which was actively exploited as a zero-day to download files. [...]

Apple Releases Urgent Updates to Patch Actively Exploited Zero-Day Vulnerabilities

The Hacker News - 20 November 2024 11:07

Apple has released security updates for iOS, iPadOS, macOS, visionOS, and its Safari web browser to address two zero-day flaws that have come under active exploitation in the wild.The flaws are listed below -CVE-2024-44308 - A vulnerability in JavaScriptCore that could lead to arbitrary code execution when processing malicious web content.

D-Link urges users to retire VPN routers impacted by unfixed RCE flaw

BleepingComputer - 19 November 2024 13:58

D-Link is warning customers to replace end-of-life VPN router models after a critical unauthenticated, remote code execution vulnerability was discovered that will not be fixed on these devices. [...]

U.S. CISA adds Progress Kemp LoadMaster, Palo Alto Networks PAN-OS and Expedition bugs to its Known Exploited Vulnerabilities catalog

Security Affairs - 19 November 2024 09:34

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds Progress Kemp LoadMaster, Palo Alto Networks PAN-OS and Expedition bugs to its Known Exploited Vulnerabilities catalog.

Threat actors and malware

New 'Helldown' Ransomware Variant Expands Attacks to VMware and Linux Systems

The Hacker News - 19 November 2024 16:10

Cybersecurity researchers have shed light on a Linux variant of a relatively new ransomware strain called Helldown, suggesting that the threat actors are broadening their attack focus.

China-linked actor's malware DeepData exploits FortiClient VPN zero-day

Scottish Cyber Coordination Centre

Security Affairs - 19 November 2024 16:05

Chinese threat actors use custom post-exploitation toolkit ‘DeepData’ to exploit FortiClient VPN zero-day and steal credentials. Volexity researchers discovered a vulnerability in Fortinet’s Windows VPN client that China-linked threat actor BrazenBamboo abused in their DEEPDATA malware.

Apple Confirms Zero-Day Attacks Hitting macOS Systems

SecurityWeek - 19 November 2024 21:39

Apple rushes out out major macOS and iOS security updates to cover a pair of vulnerabilities already being exploited in the wild.