Scottish Cyber Coordination Centre

Daily threat bulletin

28 November 2024

Vulnerabilities

Hackers exploit ProjectSend flaw to backdoor exposed servers

BleepingComputer - 27 November 2024 17:00

Threat actors are using public exploits for a critical authentication bypass flaw in ProjectSend to upload webshells and gain remote access to servers. [...]

VMware fixed five vulnerabilities in Aria Operations product

Security Affairs - 27 November 2024 15:54

Virtualization giant VMware addressed multiple vulnerabilities in its Aria Operations product that can led to privilege escalation and XSS attacks. VMware released security updates to address five vulnerabilities in its Aria Operations product. Aria Operations (formerly known as VMware vRealize Operations) is a comprehensive cloud management and operations platform developed by VMware.

Threat actors and malware

New Bootkit “Bootkitty” Targets Linux Systems via UEFI

Infosecurity Magazine - 27 November 2024 17:30

Bootkitty, the first Linux-targeting UEFI bootkit, bypassed kernel security in a proof-of-concept attack

APT-C-60 Hackers Exploit StatCounter and Bitbucket in SpyGlace Malware Campaign

The Hacker News - 27 November 2024 17:44

The threat actor known as APT-C-60 has been linked to a cyber attack targeting an unnamed organization in Japan that used a job application-themed lure to deliver the SpyGlace backdoor.That’s according to findings from JPCERT/CC, which said the intrusion leveraged legitimate services like Google Drive, Bitbucket, and StatCounter.

Russian APT Chained Firefox and Windows Zero-Days Against US and European Targets

SecurityWeek - 27 November 2024 10:19

The Russia-linked RomCom APT has been observed chaining two zero-days in Firefox and Windows for backdoor delivery.

Hackers abuse popular Godot game engine to infect thousands of PCs

Scottish Cyber Coordination Centre

BleepingComputer - 27 November 2024 17:17

Hackers have used new GodLoader malware exploiting the capabilities of the widely used Godot game engine to evade detection and infect over 17,000 systems in just three months. [...]

UK related

BIC, Starbucks, Morrisons continue recovery after Blue Yonder ransomware attack

The Record from Recorded Future News - 27 November 2024 18:34