Scottish Cyber Coordination Centre

Daily threat bulletin

16 October 2024

Vulnerabilities

CISA Warns of Active Exploitation in SolarWinds Help Desk Software Vulnerability

The Hacker News - 16 October 2024 11:24

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Tuesday added a critical security flaw impacting SolarWinds Web Help Desk (WHD) software to its Known Exploited Vulnerabilities (KEV) catalog, citing evidence of active exploitation. Tracked as CVE-2024-28987 (CVSS score: 9.1.

GitHub Patches Critical Vulnerability in Enterprise Server

SecurityWeek - 15 October 2024 18:30

A critical-severity flaw in GitHub Enterprise Server could lead to unauthorized access to the vulnerable instances.

Splunk Enterprise Update Patches Remote Code Execution Vulnerabilities

SecurityWeek - 15 October 2024 13:51

Splunk has released patches for multiple vulnerabilities in Splunk Enterprise, including two high-severity remote code execution flaws.

WordPress Jetpack plugin critical flaw impacts 27 million sites

Security Affairs - 15 October 2024 10:43

WordPress Jetpack plugin issued an update to fix a critical flaw allowing logged-in users to view form submissions by others on the same site. The maintainers of the WordPress Jetpack plugin have addressed a critical vulnerability that could allow logged-in users to access forms submitted by other users on the same site.

Threat actors and malware

EDRSilencer red team tool used in attacks to bypass security

BleepingComputer - 15 October 2024 15:47

A tool for red-team operations called EDRSilencer has been observed in malicious incidents attempting to identify security tools and mute their alerts to management consoles. [...]

New CounterSEVeillance and TDXDown Attacks Target AMD and Intel TEEs

SecurityWeek - 15 October 2024 10:40

Scottish Cyber Coordination Centre

Intel and AMD respond to new attack methods named TDXDown and CounterSEVeillance that can be used against TDX and SEV technology.

New Malware Campaign Uses PureCrypter Loader to Deliver DarkVision RAT

The Hacker News - 15 October 2024 21:50

Cybersecurity researchers have disclosed a new malware campaign that leverages a malware loader named PureCrypter to deliver a commodity remote access trojan (RAT) called DarkVision RAT.

A new Linux variant of FASTCash malware targets financial systems

Security Affairs - 15 October 2024 18:57

North Korea-linked actors deploy a new Linux variant of FASTCash malware to target financial systems, researcher HaxRob revealed. The cybersecurity researcher HaxRob analyzed a new variant of the FASTCash “payment switch” malware which targets Linux systems.

Researchers Uncover Hijack Loader Malware Using Stolen Code-Signing Certificates

The Hacker News - 15 October 2024 13:13

Cybersecurity researchers have disclosed a new malware campaign that delivers Hijack Loader artifacts that are signed with legitimate code-signing certificates.French cybersecurity company HarfangLab, which detected the activity at the start of the month, said the attack chains aim to deploy an information stealer known as Lumma.