Scottish Cyber Coordination Centre

Daily threat bulletin

24 October 2024

Vulnerabilities

Fortinet warns of new critical FortiManager flaw used in zero-day attacks

BleepingComputer - 23 October 2024 12:05

Fortinet publicly disclosed today a critical FortiManager API vulnerability, tracked as CVE-2024-47575, that was exploited in zero-day attacks to steal sensitive files containing configurations, IP addresses, and credentials for managed devices. [...]

CISA Warns of Active Exploitation of Microsoft SharePoint Vulnerability (CVE-2024-38094)

The Hacker News - 23 October 2024 19:24

A high-severity flaw impacting Microsoft SharePoint has been added to the Known Exploited Vulnerabilities (KEV) catalog by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Tuesday, citing evidence of active exploitation.The vulnerability, tracked as CVE-2024-38094 (CVSS score: 7.2), has been described as a deserialization vulnerability impacting SharePoint.

The Crypto Game of Lazarus APT: Investors vs. Zero-days

Securelist - 23 October 2024 12:00

Kaspersky GReAT experts break down the new campaign of Lazarus APT which uses social engineering and exploits a zero-day vulnerability in Google Chrome for financial gain.

Threat actors and malware

New Grandoreiro Banking Malware Variants Emerge with Advanced Tactics to Evade Detection

The Hacker News - 24 October 2024 00:03

New variants of a banking malware called Grandoreiro have been found to adopt new tactics in an effort to bypass anti-fraud measures, indicating that the malicious software is continuing to be actively developed despite law enforcement efforts to crack down on the operation.

Perfctl malware strikes again as crypto-crooks target Docker Remote API servers

The Register - 24 October 2024 03:30

Attacks on unprotected servers reach 'critical level'. An unknown attacker is abusing exposed Docker Remote API servers to deploy perfctl cryptomining malware on victims' systems, according to Trend Micro researchers.

Scottish Cyber Coordination Centre

New Malware WarmCookie Targets Users with Malicious Links

Infosecurity Magazine - 23 October 2024 17:00

WarmCookie malware, aka BadSpace, spreads via malspam, malvertising and enables persistent access.

Embargo Ransomware Gang Deploys Customized Defense Evasion Tools

Infosecurity Magazine - 23 October 2024 16:02

The recently discovered Embargo ransomware group is using Rust-based custom tools to overcome victims' security defenses, ESET researchers have observed.

Avast Releases Free Decryptor for Mallox Ransomware

SecurityWeek - 23 October 2024 14:59

Avast has released a decryptor for the Mallox ransomware after identifying a weakness in its cryptographic schema.

NotLockBit Ransomware Can Target macOS Devices

SecurityWeek - 23 October 2024 12:53

A file-encrypting malware family posing as the LockBit ransomware has been observed targeting macOS systems.