Scottish Cyber Coordination Centre

Daily threat bulletin

11 April 2024

Vulnerabilities

Fortinet fixed a critical remote code execution bug in FortiClientLinux

Security Affairs - 10 April 2024 19:15

Fortinet addressed multiple issues in FortiOS and other products, including a critical remote code execution flaw in FortiClientLinux. Fortinet fixed a dozen vulnerabilities in multiple products, including a critical-severity remote code execution (RCE) issue, tracked as CVE-2023-45590 (CVSS score of 9.4), in FortiClientLinux. The vulnerability is an Improper Control of Generation of Code ('Code Injection') […]

Researchers Uncover First Native Spectre v2 Exploit Against Linux Kernel

The Hacker News - 10 April 2024 15:56

Cybersecurity researchers have disclosed what they say is the "first native Spectre v2 exploit" against the Linux kernel on Intel systems that could be exploited to read sensitive data from the memory.The exploit, called Native Branch History Injection (BHI), can be used to leak arbitrary kernel memory at 3.5 kB/sec by bypassing existing Spectre v2/BHI mitigations, researchers from Systems and

New Spectre v2 attack impacts Linux systems on Intel CPUs

BleepingComputer - 10 April 2024 14:19

Researchers have demonstrated the "first native Spectre v2 exploit" for a new speculative execution side-channel flaw that impacts Linux systems running on many modern Intel processors. […]

Threat actors and malware

Malicious Visual Studio projects on GitHub push Keyzetsu malware

BleepingComputer - 10 April 2024 08:00

Threat actors are abusing GitHub automation features and malicious Visual Studio projects to push a new variant of the "Keyzetsu" clipboard-hijacking malware and steal cryptocurrency payments. […]

Raspberry Robin Returns: New Malware Campaign Spreading Through WSF Files

The Hacker News - 10 April 2024 19:40

Cybersecurity researchers have discovered a new Raspberry Robin campaign wave that propagates the malware through malicious Windows Script Files (WSFs) since March 2024.”Historically, Raspberry Robin was known to spread through removable media like USB drives, but over time its distributors have experimented with other initial infection vectors,” HP Wolf Security researcher Patrick Schläpfer&

Cagey Phishing Campaign Delivers Multiple RATs to Steal Windows Data

darkreading - 10 April 2024 15:45

Various anti-detection features, including the use of the ScrubCrypt antivirus-evasion tool, fuel an attack that aims to take over Microsoft Windows machines.

Rhadamanthys Malware Deployed By TA547 Against German Targets

Infosecurity Magazine - 10 April 2024 17:00

Proofpoint said this is the first time the threat actor has been seen using LLM-generated PowerShell scripts

CISA Releases Malware Next-Gen Analysis System for Public Use

SecurityWeek - 10 April 2024 20:40

CISA’s Malware Next-Gen system is now available for any organization to submit malware samples and other suspicious artifacts for analysis.The post CISA Releases Malware Next-Gen Analysis System for Public Use appeared first on SecurityWeek.