Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

15 April 2025

Vulnerabilities

Gladinet's Triofox and CentreStack Under Active Exploitation via Critical RCE Vulnerability

The Hacker News - 15 April 2025 11:09

A recently disclosed security flaw in Gladinet CentreStack also impacts its Triofox remote access and collaboration solution, according to Huntress, with seven different organizations compromised to date.Tracked as CVE-2025-30406 (CVSS score: 9.0), the vulnerability refers to the use of a hard-coded cryptographic key that could expose internet-accessible servers to remote code execution attacks.

Fortinet Zero-Day Bug May Lead to Arbitrary Code Execution

darkreading - 14 April 2025 18:20

A threat actor posted about the zero-day exploit on the same day that Fortinet published a warning about known vulnerabilities under active exploitation.

Major WordPress Plugin Flaw Exploited in Under 4 Hours

Infosecurity Magazine - 14 April 2025 16:00

Flaw in SureTriggers plugin allows unauthenticated users to create admin accounts on WordPress sites

Threat actors and malware

New ResolverRAT malware targets pharma and healthcare orgs worldwide

BleepingComputer - 14 April 2025 13:40

A new remote access trojan (RAT) called 'ResolverRAT' is being used against organizations globally, with the malware used in recent attacks targeting the healthcare and pharmaceutical sectors. [...]

Phishing Campaigns Use Real-Time Checks to Validate Victim Emails Before Credential Theft

The Hacker News - 14 April 2025 19:54

Cybersecurity researchers are calling attention to a new type of credential phishing scheme that ensures that the stolen information is associated with valid online accounts.The technique has been codenamed precision-validating phishing by Cofense, which it said employs real-time email validation so that only a select set of high-value targets are served the fake login screens.

Threat Actor Allegedly Selling Fortinet Firewall Zero-Day Exploit

SecurityWeek - 14 April 2025 14:48

A threat actor claims to offer a zero-day exploit for an unauthenticated remote code execution vulnerability in Fortinet firewalls.

UK related

How much vital UK infrastructure does China own?

BBC News - 14 April 2025 17:43

BBC Verify looks at what we know about the extent of Chinese investment in the UK economy.