Scottish Cyber Coordination Centre

Daily Threat Bulletin

21 August 2024

Vulnerabilities

Hackers use PHP exploit to backdoor Windows systems with new malware

BleepingComputer - 20 August 2024 14:49

Unknown attackers have deployed a newly discovered backdoor dubbed Msupedge on a university's Windows systems in Taiwan, likely by exploiting a recently patched PHP remote code execution vulnerability (CVE-2024-4577).

GiveWP WordPress Plugin Vulnerability Puts 100,000+ Websites at Risk

The Hacker News - 21 August 2024 11:05

A maximum-severity security flaw has been disclosed in the WordPress GiveWP donation and fundraising plugin that exposes more than 100,000 websites to remote code execution attacks. The flaw, tracked as CVE-2024-5932 (CVSS score: 10.0), impacts all versions of the plugin prior to version 3.14.2, which was released on August 7, 2024.

Azure Kubernetes Bug Lays Open Cluster Secrets

darkreading - 20 August 2024 21:55

Vulnerability gave attackers with access to a pod a way to obtain credentials and other secrets.

Cisco, Microsoft Disagree on Severity of macOS App Vulnerabilities

SecurityWeek - 20 August 2024 12:31

Multiple vulnerabilities in Microsoft applications for macOS could be exploited to send emails, leak sensitive information, and escalate privileges.

F5 Patches High-Severity Vulnerabilities in BIG-IP, NGINX Plus

SecurityWeek - 20 August 2024 09:55

F5's latest quarterly security notification includes nine advisories, including four for high-severity vulnerabilities in BIG-IP and NGINX Plus.

Threat actors and malware

IRGC-Linked Hackers Package Modular Malware in Monolithic Trojan

darkreading - 20 August 2024 10:00

Charming Kitten goes retro and consolidates its backdoor into a tighter package, abandoning the malware framework trend.

Scottish Cyber Coordination Centre

Novel Phishing Method Used in Android/iOS Financial Fraud Campaigns

Infosecurity Magazine - 20 August 2024 18:00

ESET detected a new phishing technique using progressive web applications (PWAs) as part of a large-scale mobile financial scam.

'Styx Stealer' malware developer accidentally exposes personal info to researchers in 'critical opsec error'

The Record from Recorded Future News - 20 August 2024 14:02

A suspected developer of a new malware strain called Styx Stealer made a "significant operational security error" and leaked data from his computer, including details about clients and earnings, researchers have found.