Scottish Cyber Coordination Centre

Daily Threat Bulletin

11 February 2025

Vulnerabilities

XE Hacker Group Exploits VeraCore Zero-Day to Deploy Persistent Web Shells

The Hacker News - 10 February 2025 11:44

Threat actors have been observed exploiting multiple security flaws in various software products, including Progress Telerik UI for ASP.NET AJAX and Advantive VeraCore, to drop reverse shells and web shells, and maintain persistent remote access to compromised systems. The zero-day exploitation of security flaws in VeraCore has been attributed to a threat actor known as XE Group.

Apple fixes iPhone and iPad bug exploited in ‘extremely sophisticated attacks’

Security Affairs - 10 February 2025 23:41

Apple released emergency security updates to address a zero-day vulnerability, tracked as CVE-2025-24200, that the company believes was exploited in ‘extremely sophisticated’ targeted attacks.

Zimbra Releases Security Updates for SQL Injection, Stored XSS, and SSRF Vulnerabilities

The Hacker News - 10 February 2025 15:39

Zimbra has released software updates to address critical security flaws in its Collaboration software that, if successfully exploited, could result in information disclosure under certain conditions. The vulnerability, tracked as CVE-2025-25064, carries a CVSS score of 9.8 out of a maximum of 10.0.

Over 12,000 KerioControl firewalls exposed to exploited RCE flaw

BleepingComputer - 10 February 2025 19:58

Over twelve thousand GFI KerioControl firewall instances are exposed to a critical remote code execution vulnerability tracked as CVE-2024-52875.

Orthanc Server Vulnerability Poses Risk to Medical Data, Healthcare Operations

SecurityWeek - 10 February 2025 13:53

A critical vulnerability found in Orthanc servers can pose a serious risk to medical data and healthcare operations.

Threat actors and malware

DragonRank Exploits IIS Servers with BadIIS Malware for SEO Fraud and Gambling Redirects

The Hacker News - 10 February 2025 16:14

Threat actors have been observed targeting Internet Information Services (IIS) servers in Asia as part of a search engine optimization (SEO) manipulation campaign designed to install BadIIS malware.

Magecart Attackers Abuse Google Ad Tool to Steal Data

darkreading - 10 February 2025 16:19

Attackers are smuggling payment card-skimming malicious code into checkout pages on Magento-based e-commerce sites by abusing the Google Tag Manager ad tool.

Police arrests 4 Phobos ransomware suspects, seizes 8Base sites

BleepingComputer - 10 February 2025 12:51

A global law enforcement operation targeting the Phobos ransomware gang has led to the arrest of four suspected hackers in Phuket, Thailand, and the seizure of 8Base's dark web sites.

UK Specific

Experts Dismayed at UK’s Apple Decryption Demands

Infosecurity Magazine - 10 February 2025 11:30

Security and privacy experts have questioned a new demand from the UK Home Office on Apple’s encrypted iCloud service

UK armed forces fast-tracking cyber warriors to defend digital front lines

The Register - 10 February 2025 10:30

The UK's Ministry of Defence (MoD) is fast-tracking cybersecurity specialists in a bid to fortify its protection against increasing attacks.