Scottish
Cyber
Coordination
Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

9 January 2023

Vulnerabilities

Cacti Monitoring Tool Spiked by Critical SQL Injection Vulnerability

Dark Reading - January 8 2024

A critical vulnerability in the Cacti Web-based open source framework for monitoring network performance gives attackers a way to disclose Cacti's entire database contents — presenting a prickly risk for organizations. Thousands of websites use Cacti to collect network performance information such as that related to bandwidth utilization, CPU and memory usage, and disk I/O — from devices such as routers, switches, and servers.

CISA Adds Six Known Exploited Vulnerabilities to Catalog

CISA Current Activity - January 8 2024

CISA has added six new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. CVE-2023-38203 Adobe ColdFusion Deserialization of Untrusted Data Vulnerability CVE-2023-29300 Adobe ColdFusion Deserialization of Untrusted Data Vulnerability CVE-2023-27524 Apache Superset Insecure Default Initialization of Resource Vulnerability CVE-2023-41990 Apple Multiple Products Code Execution Vulnerability CVE-2016-20017 D-Link DSL-2750B Devices Command Injection Vulnerability CVE-2023-23752 Joomla! Improper Access Control Vulnerability.

Apache OFBiz zero-day pummeled by exploit attempts after disclosure

The Register - Security - January 8 2024

SonicWall says it has observed thousands of daily attempts to exploit an Apache OFBiz zero-day for nearly a fortnight.

UK cyber

Optionis (now Caroola Group) hit with ICO reprimand over ransomware attack from 2022

Contractor UK - January 8 2024

TLP CLEAR: Disclosure is not limited

The Information Commissioner’s Office has reprimanded Optionis, now Caroola Group, over what has been called ‘one of the largest ever ransomware attacks on the accounting industry.’

British Library: Finances remain healthy as ransomware recovery continues

The Register - Security - RSS - January 8 2024

Authors continue to lose out on owed payments as rebuild of digital services drags on The British Library is denying reports suggesting the recovery costs for its 2023 ransomware attack may reach highs of nearly $9 million as work to restore services.

Malware and threat actors

Long-existing Bandook RAT targets Windows machines

Security Affairs - January 8 2024

A new variant of the Bandook remote access trojan (RAT) was spotted in attacks aimed at Windows machines. Reseachers from Fortinet observed a new variant of a remote access trojan dubbed Bandook that has been used in phishing attacks against Windows users. Bandook has been active since 2007, it has been continuously developed since then and was employed in several campaigns by different threat actors.

Details of a new, novel advanced malware attack using Microsoft Office

Forcepoint.com - January 8 2024