Scottish Cyber Coordination Centre

Daily threat bulletin

6 September 2024

Vulnerabilities

Apache fixes critical OFBiz remote code execution vulnerability

BleepingComputer - 05 September 2024 18:33

Apache has fixed a critical security vulnerability in its open-source OFBiz (Open For Business) software, which could allow attackers to execute arbitrary code on vulnerable Linux and Windows servers. [...]

LiteSpeed Cache bug exposes 6 million WordPress sites to takeover attacks

BleepingComputer - 05 September 2024 13:58

Yet, another critical severity vulnerability has been discovered in LiteSpeed Cache, a caching plugin for speeding up user browsing in over 6 million WordPress sites. [...]

Veeam fixed a critical flaw in Veeam Backup & Replication software

Security Affairs - 05 September 2024 20:57

Veeam addressed 18 high and critical severity flaws in Veeam Backup & Replication, Service Provider Console, and One. Veeam security updates to address multiple vulnerabilities impacting its products, the company fixed 18 high and critical severity flaws in Veeam Backup & Replication, Service Provider Console, and One.

Cisco Fixes Two Critical Flaws in Smart Licensing Utility to Prevent Remote Attacks

The Hacker News - 05 September 2024 11:10

Cisco has released security updates for two critical security flaws impacting its Smart Licensing Utility that could allow unauthenticated, remote attackers to elevate their privileges or access sensitive information.

Threat actors and malware

Earth Lusca adds multiplatform malware KTLVdoor to its arsenal

Security Affairs - 05 September 2024 14:15

The Chinese-speaking threat actor Earth Lusca used the new backdoor KTLVdoor in an attack against a trading company in China. Trend Micro Researchers spotted the Chinese-speaking threat actor Earth Lusca using a new multiplatform backdoor called KTLVdoor.

Malware Attackers Using MacroPack to Deliver Havoc, Brute Ratel, and PhantomCore

The Hacker News - 05 September 2024 14:15

Scottish Cyber Coordination Centre

Threat actors are likely employing a tool designated for red teaming exercises to serve malware, according to new findings from Cisco Talos.

Chinese 'Tropic Trooper' APT Targets Mideast Governments

darkreading - 05 September 2024 21:39

In the past, the group has targeted different sectors in East and Southeast Asia, but recently has pivoted its focus to the Middle East, specifically to entities that publish human rights studies.