Scottish Cyber Coordination Centre

Daily threat bulletin

7 June 2024

Vulnerabilities

Hackers exploit 2018 ThinkPHP flaws to install 'Dama' web shells

BleepingComputer - 06 June 2024 18:26

Chinese threat actors are targeting ThinkPHP applications vulnerable to CVE-2018-20062 and CVE-2019-9082 to install a persistent web shell named Dama.

Attacks Surge on Check Point's Recent VPN Zero-Day Flaw

darkreading - 06 June 2024 21:16

One monitoring firm has detected exploitation attempts targeting CVE-2024-24919 from more than 780 unique IP addresses in the past week.

POC exploit code published for 9.8-rated Apache HugeGraph RCE flaw

The Register - 07 June 2024 02:16

You upgraded when this was fixed in April, right? Right?? If you haven't yet upgraded to version 1.3.0 of Apache HugeGraph, now's a good time because at least two proof-of-concept exploits for a CVSS 9.8-rated remote command execution bug in the open-source graph database have been made public.

7-year-old Oracle WebLogic bug under active exploitation

The Register - 06 June 2024 11:37

Experts say Big Red will probably re-release patch in an upcoming cycle. A seven-year-old Oracle vulnerability is the latest to be added to CISA's Known Exploited Vulnerability (KEV) catalog, meaning the security agency considers it a significant threat to federal government.

Vulnerabilities Patched in Kiuwan Code Security Products After Long Disclosure Process

SecurityWeek - 06 June 2024 13:06

It took code security firm Kiuwan nearly two years to patch several serious vulnerabilities found in its SAST products. The post Vulnerabilities Patched in Kiuwan Code Security Products After Long Disclosure Process appeared first on SecurityWeek.

Threat actors and malware

New Fog ransomware targets US education sector via breached VPNs

BleepingComputer - 06 June 2024 15:29

A new ransomware operation named 'Fog' launched in early May 2024, using compromised VPN credentials to breach the networks of educational organizations in the U.S. [...]

Muhstik Botnet Exploiting Apache RocketMQ Flaw to Expand DDoS Attacks

The Hacker News - 06 June 2024 19:44

The distributed denial-of-service (DDoS) botnet known as Muhstik has been observed leveraging a now-patched security flaw impacting Apache RocketMQ to co-opt susceptible servers and expand its scale.

Hackers Target Python Developers with Fake "Crytic-Compilers" Package on PyPI

The Hacker News - 06 June 2024 12:19

Cybersecurity researchers have discovered a malicious Python package uploaded to the Python Package Index (PyPI) repository that's designed to deliver an information stealer called Lumma (aka LummaC2).

Chinese Hackers Exploit Old ThinkPHP Vulnerabilities in New Attacks

SecurityWeek - 06 June 2024 17:52

Akamai warns that a Chinese threat actor is exploiting years-old remote code execution vulnerabilities in ThinkPHP in new attacks.The post Chinese Hackers Exploit Old ThinkPHP Vulnerabilities in New Attacks appeared first on SecurityWeek.