Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

19 March 2024

Vulnerabilities

Remove WordPress miniOrange plugins, a critical flaw can allow site takeover

Security Affairs - March 18 2024

A critical vulnerability in WordPress miniOrange's Malware Scanner and Web Application Firewall plugins can allow site takeover. On March 1st, 2024, WordPress security firm Wordfence received a submission for a Privilege Escalation vulnerability in miniOrange's Malware Scanner as part of the company Bug Bounty initiative Extravaganza.

FortiClient Endpoint Management Server (EMS) SQL Injection Vulnerability (CVE-2023-48788)

Qualys Threat Protection - March 19 2024

Fortinet addressed a critical severity vulnerability impacting the FortiClient Enterprise Management Server. Tracked as CVE-2023-48788, the vulnerability may allow an attacker to achieve code execution on affected systems.

PoC exploit for critical RCE flaw in Fortra FileCatalyst transfer tool released

Security Affairs - March 18 2024

Fortra addressed a critical remote code execution vulnerability impacting its FileCatalyst file transfer product. Fortra has released updates to address a critical vulnerability, tracked as CVE-2024-25153 (CVSS score 9.8) impacting its FileCatalyst file transfer solution. A remote, unauthenticated attacker can exploit their vulnerability to execute arbitrary code on impacted servers.

Malware and threat actors

CISA: Healthcare Organizations Should Be Wary of Increased Ransomware Attacks by ALPHV Blackcat

KnowBe4 - Blog - RSS - March 18 2024

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

A joint cybersecurity advisory published last week discusses ransomware attack impacts on healthcare, along with ALPHV's attack techniques, indicators of compromise (IoCs) and proper response actions.

StopCrypt: Most widely distributed ransomware evolves to evade detection
MalwareTips.com - March 19 2024

A new variant of StopCrypt ransomware (aka STOP) was spotted in the wild, employing a multi-stage execution process that involves shellcodes to evade security tools.

New ShadowSyndicate ransomware attacks involve aiohttp flaw exploitation
SC Magazine US - March 18 2024

BleepingComputer reports that intrusions targeting servers impacted by the high-severity direct traversal aiohttp Python library vulnerability, tracked as CVE-2024-23334, have been increasingly deployed by suspected ransomware-as-as-service affiliate ShadowSyndicate since the end of February, or a month after fixes for the security issue was addressed.

Chinese Earth Krahang hackers breach 70 orgs in 23 countries
BleepingComputer.com - March 18 2024

A sophisticated hacking campaign attributed to a Chinese Advanced Persistent Threat (APT) group known as 'Earth Krahang' has breached 70 organizations and targeted at least 116 across 45 countries. [...]