Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

22 February 2024

Vulnerabilities

ConnectWise exploit could spur ‘ransomware free-for-all,’ expert warns
SC Magazine US - February 21 2024

A critical ConnectWise ScreenConnect vulnerability that puts thousands of servers at risk of takeover is actively being exploited in the wild, ConnectWise said Tuesday. ConnectWise released a security fix for ScreenConnect 23.9.7 on Monday, disclosing two vulnerabilities, including a critical bug with a maximum CVSS score of 10.

Joomla fixes XSS flaws that could expose sites to RCE attacks
Bleeping Computer - February 21 2024

Five vulnerabilities have been discovered in the Joomla content management system that could be leveraged to execute arbitrary code on vulnerable websites. The vendor has addressed the security issues, which impact multiple versions of Joomla, and fixes are present in versions 5.0.3 and also 4.4.3 of the CMS.

New Wi-Fi Vulnerabilities Expose Android and Linux Devices to Hackers
The Hacker News - February 21 2024

Cybersecurity researchers have identified two authentication bypass flaws in open-source Wi-Fi software found in Android, Linux, and ChromeOS devices that could trick users into joining a malicious clone of a legitimate network or allow an attacker to join a trusted network without a password.

CISA, EPA, and FBI Release Top Cyber Actions for Securing Water Systems
CISA Current Activity - February 21 2024

Today, CISA, the Environmental Protection Agency (EPA), and the Federal Bureau of Investigation (FBI) released the joint fact sheet Top Cyber Actions for Securing Water Systems.

Mozilla Releases Security Updates for Firefox and Thunderbird
CISA Current Activity - February 21 2024

Mozilla released security updates to address vulnerabilities in Firefox, Firefox ESR, and Thunderbird. A cyber threat actor could exploit one of these vulnerabilities to take control of an affected system.

Zardoor Backdoor Alert: Threat Actors Target Islamic Charity
Security Bloggers Network - February 21 2024

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

In recent cyber threat intelligence developments, an unnamed Islamic non-profit organization based in Saudi Arabia has fallen victim to a covert cyber-espionage campaign employing a previously unknown backdoor named Zardoor.

Malware and threat actors

Mustang Panda Targets Asia with Advanced PlugX Variant DOPLUGS
The Hacker News - February 21 2024

The China-linked threat actor known as Mustang Panda has targeted various Asian countries using a variant of the PlugX (aka Korplug) backdoor dubbed DOPLUGS.