Scottish Cyber Coordination Centre

Daily threat bulletin

13 August 2024

Vulnerabilities

A FreeBSD flaw could allow remote code execution, patch it now!

Security Affairs - 12 August 2024 18:38

FreeBSD Project maintainers addressed a high-severity flaw in OpenSSH that could allow remote code execution with elevated privileges. The maintainers of the FreeBSD Project have released urgent security updates to address a high-severity flaw, tracked as CVE-2024-7589, (CVSS score of 7.4) in OpenSSH. A remote attacker could exploit the vulnerability to execute arbitrary code with elevated [...]

Microsoft found OpenVPN bugs that can be chained to achieve RCE and LPE

Security Affairs - 12 August 2024 08:01

Microsoft found four bugs in OpenVPN that could be chained to achieve remote code execution and local privilege escalation. During the Black Hat USA 2024 conference, Microsoft researchers disclosed multiple medium-severity bugs in the open-source project OpenVPN that could be chained to achieve remote code execution (RCE) and local privilege escalation (LPE).

Industrial Remote Access Tool Ewon Cosy+ Vulnerable to Root Access Attacks

The Hacker News - 12 August 2024 13:27

Security vulnerabilities have been disclosed in the industrial remote access solution Ewon Cosy+ that could be abused to gain root privileges to the devices and stage follow-on attacks. The elevated access could then be weaponized to decrypt encrypted firmware files and encrypted data such as passwords in configuration files, and even get correctly signed X.509 VPN certificates.

CLFS Bug Crashes Even Updated Windows 10, 11 Systems

darkreading - 12 August 2024 19:00

A quick and easy exploit for crashing Windows computers has no fix yet nor really any way to mitigate its effects.

Threat actors and malware

FBI disrupts the Dispossessor ransomware operation, seizes servers

BleepingComputer - 12 August 2024 18:48

The FBI announced on Monday that it seized the servers and websites of the Radar/Dispossessor ransomware operation following a joint international investigation. [...]

Scottish Cyber Coordination Centre

Ukraine Warns of New Phishing Campaign Targeting Government Computers

The Hacker News - 13 August 2024 11:42

The Computer Emergency Response Team of Ukraine (CERT-UA) has warned of a new phishing campaign that masquerades as the Security Service of Ukraine to distribute malware capable of remote desktop access.The agency is tracking the activity under the name UAC-0198.

How Phishing Attacks Adapt Quickly to Capitalize on Current Events

The Hacker News - 12 August 2024 17:50

In 2023, no fewer than 94 percent of businesses were impacted by phishing attacks, a 40 percent increase compared to the previous year, according to research from Egress.What's behind the surge in phishing? One popular answer is AI – particularly generative AI, which has made it trivially easier for threat actors to craft content that they can use in phishing campaigns, like malicious emails.