Scottish Cyber Coordination Centre

Daily threat bulletin

20 June 2024

Vulnerabilities

Google Chrome 126 update addresses multiple high-severity flaws

Security Affairs - 19 June 2024 19:47

Google released Chrome 126 update that addresses a high-severity vulnerability demonstrated at the TyphoonPWN 2024 hacking competition. Google has issued a Chrome 126 security update, addressing six vulnerabilities, including a flaw, tracked as CVE-2024-6100 which was demonstrated during the SSD Secure Disclosure's TyphoonPWN 2024.

Mailcow Mail Server Flaws Expose Servers to Remote Code Execution

The Hacker News - 19 June 2024 14:06

Two security vulnerabilities have been disclosed in the Mailcow open-source mail server suite that could be exploited by malicious actors to achieve arbitrary code execution on susceptible instances.Both shortcomings impact all versions of the software prior to version 2024-04, which was released on April 4, 2024.

CISA Warns of PoC Exploit for Vulnerability in RAD SecFlow-2 Industrial Switch

SecurityWeek - 19 June 2024 11:48

CISA has notified RAD after finding a PoC exploit targeting a high-severity vulnerability in an outdated industrial switch.

Threat actors and malware

Cryptojacking campaign targets exposed Docker APIs

Security Affairs - 19 June 2024 08:31

A malware campaign targets publicly exposed Docker API endpoints to deliver cryptocurrency miners and other payloads. Researchers at Datadog uncovered a new cryptojacking campaign linked to the attackers behind Spinning YARN campaign.

Experts Uncover New Evasive SquidLoader Malware Targeting Chinese Organizations

The Hacker News - 20 June 2024 13:04

Cybersecurity researchers have uncovered a new evasive malware loader named SquidLoader that spreads via phishing campaigns targeting Chinese organizations. AT&T LevelBlue Labs, which first observed the malware in late April 2024, said it incorporates features that are designed to thwart static and dynamic analysis and ultimately evade detection.

Email obfuscation tactics elude security protections

Scottish Cyber Coordination Centre

Security Magazine - 19 June 2024 13:00

Threat researchers have uncovered newly evolving email obfuscation techniques that are designed to evade modern security controls.

‘ONNX’ MFA Bypass Targets Microsoft 365 Accounts

darkreading - 19 June 2024 18:20

The service, likely a rebrand of a previous operation called ‘Caffeine,’ mainly targets financial institutions in the Americas and EMEA and uses malicious QR codes and other advanced evasion tactics.

That PowerShell ‘fix’ for your root cert ‘problem’ is a malware loader in disguise

The Register - 19 June 2024 08:27

Control-C, Control-V, Enter ... Hell Crafty criminals are targeting thousands of orgs around the world in social-engineering attacks that use phony error messages to trick users into running malicious PowerShell scripts.