Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

25 March 2024

Vulnerabilities

F5, ScreenConnect vulnerabilities leveraged in global Chinese cyberattacks

SC Magazine US - March 22 2024

Attacks exploiting the widely-known F5 BIG-IP and ConnectWise ScreenConnect vulnerabilities, tracked as CVE-2023-46747 and CVE-2024-1709, respectively, have been deployed by suspected Chinese state-backed threat actor UNC5174 since late last year, reports The Record, a news site by cybersecurity firm Recorded Future. UNC5174, which is believed to be an ex-member of Chinese hacktivist groups Genesis Day and Dawn Calvary, leveraged CVE-2023-46747, to compromise U.S. defense contractors, UK government organizations, and Asian entities in October and November before infiltrating hundreds more organizations, most of which are in the U.S. and Canada, in intrusions exploiting CVE-2024-1709 last month, according to a report from Mandiant.

Mozilla fixes two Firefox zero-day bugs exploited at Pwn2Own

BleepingComputer.com - March 22 2024

Mozilla has released security updates to fix two zero-day vulnerabilities in the Firefox web browser exploited during the Pwn2Own Vancouver 2024 hacking competition. [...]

Fortinet Warning: another Critical RCE Flaw

Red Sky Alliance - X-Industry - RSS - March 23 2024

Our friends at Fortinet, hxxps://www[.]fortinet[.]com has patched a critical Remote Code Execution (RCE) vulnerability in its FortiClient Enterprise Management Server (EMS) for managing endpoint devices. The flaw, identified as CVE-2024-48788, stems from an SQL injection error in a direct-attached storage component of the server. It gives unauthenticated attackers a way to execute arbitrary code and commands with system admin privileges on affected systems, using specially crafted requests.[1] Fortinet gave the vulnerability a severity rating of 9.3 out of 10 on the CVSS rating scale and the National Vulnerability Database itself has assigned it a near maximum score of 9.8.

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Malware and threat actors

Large-scale Sign1 malware campaign already infected 39,000+ WordPress sites

Security Affairs - March 23 2024

A large-scale malware campaign, tracked as Sign1, has already compromised 39,000 WordPress sites in the last six months. Sucurity researchers at Sucuri spotted a malware campaign, tracked as Sign1, which has already compromised 39,000 WordPress sites in the last six months. The experts discovered that threat actors compromised the websites implanting malicious JavaScript injections that redirect visitors to malicious websites.

RaaS Groups Go Recruiting in Wake of LockBit, BlackCat Takedowns

Security Bloggers Network - March 22 2024

The effects of the recent high-profile disruptions of LockBit's and BlackCat ransomware operations by law enforcement agencies are rippling through the dark web, with smaller threat gangs looking to scoop up the larger groups' disaffected affiliates. Law enforcement agencies in the United States, the UK, and elsewhere in recent years have aggressively targeted the most.. The post RaaS Groups Go Recruiting in Wake of LockBit, BlackCat Takedowns appeared first on Security Boulevard.

Iranian TA450 Group Tries Out New Tactics on Israelis

BankInfoSecurity - March 23 2024

Proofpoint Researchers Say Beware of Phishing Emails, Embedded Links in PDFs
Iran-aligned threat actor TA450, also called MuddyWater, is using fake salary, compensation and financial incentive emails to trick Israeli employees at multi-national organizations into clicking malicious links, according to researchers at security firm Proofpoint.

Russia-linked APT29 targeted German political parties with WINELOADER backdoor

Security Affairs - March 23 2024

Russia-linked threat actors employ the WINELOADER backdoor in recent attacks targeting German political parties. In late February, Mandiant researchers spotted the Russia-linked group APT29 using a new variant of the WINELOADER backdoor to target German political parties with a CDU-themed lure. This is the first time Mandiant observed the APT29 subcluster targeting political parties, suggesting an emerging interest beyond the typical targeting of diplomatic missions. Targeted entities received phishing emails disguised as invitations to a dinner reception on March 1, featuring the logo of the German political party Christian Democratic Union (CDU). The phishing emails, written in German, included a link that led to a malicious ZIP file hosted on a compromised website.