Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

11 March 2024

Vulnerabilities

Response to ScreenConnect’s Recent Zero-day Vulnerability Exploitation
Security Boulevard - RSS - March 8 2024

AttackIQ has released a new assessment template in response to the recent wave of zero-day vulnerability exploits affecting ConnectWise's ScreenConnect software. This assessment template comprises the various Tactics, Techniques, and Procedures (TTPs)

Unauthenticated Stored XSS Vulnerability Patched in Ultimate Member WordPress Plugin
Wordfence - RSS - March 8 2024

On February 28th, 2024, during our second Bug Bounty Extravaganza, we received a submission for an unauthenticated stored Cross-Site Scripting (XSS) vulnerability in Ultimate Member, a WordPress plugin with more than 200,000+ active installations. This vulnerability can be leveraged to inject malicious web scripts. Props to stealthcopter who discovered and responsibly reported this vulnerability through the Wordfence Bug Bounty Program.

Exploit Targets Critical Vulnerability in JetBrains’ TeamCity, Company Advises Immediate Update
Tech-Wreck InfoSec Blog - March 9 2024

A critical vulnerability, identified as **CVE-2024-27198**, has been discovered in JetBrains' TeamCity On-Premises CI/CD solution, posing a significant security threat that allows remote unauthenticated attackers to gain administrative control of the server. Here's what you need to know. Tell me more about the critical vulnerability in JetBrains' TeamCity JetBrains is a company that creates tools for software developers and project

Malware and threat actors

Threat actors breached two crucial systems of the US CISA
Security Affairs - March 9 2024

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Threat actors hacked the systems of the Cybersecurity and Infrastructure Security Agency (CISA) by exploiting Ivanti flaws. The US Cybersecurity and Infrastructure Security Agency (CISA) agency was hacked in February, the Recorded Future News first reported. In response to the security breach, the agency had to shut down two crucial systems, as reported by a CISA spokesperson and US officials with knowledge of the incident, according to CNN.

Chinese Cyberspies Target Tibetans via Watering Hole, Supply Chain Attacks
SecurityWeek RSS Feed - March 8 2024

Chinese APT Evasive Panda compromises a software developer's supply chain to target Tibetans with malicious downloaders. The post Chinese Cyberspies Target Tibetans via Watering Hole, Supply Chain Attacks appeared first on SecurityWeek.

Threat Group Assessment: Muddled Libra (Updated)
Unit42 Palo Alto - RSS - March 8 2024

Muddled Libra continues to evolve. From social engineering to adaptation of new technologies, significant time is spent breaking down organizational defenses. The post Threat Group Assessment: Muddled Libra (Updated) appeared first on Unit 42.

Russia-linked Midnight Blizzard breached Microsoft systems again
Security Affairs - March 8 2024

Microsoft revealed that Russia-linked APT group Midnight Blizzard recently breached its internal systems and source code repositories. Microsoft published an update on the attack that hit the company on January 12, 2024, the IT giant revealed that the Russia-linked Midnight Blizzard recently breached again its internal systems and source code repositories.

UK government’s ransomware failings leave country ‘exposed and unprepared’
Record by Recorded Future - March 11 2024

The British government has been accused by a parliamentary committee of taking the "ostrich strategy" by burying its head in the sand over the "large and imminent" national cyber threat posed by ransomware.

Swiss cheese security? Play ransomware gang milks government of 65,000 files
The Register - Security - RSS - March 8 2024

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Classified docs, readable passwords, and thousands of personal information nabbed in Xplain breach The Swiss government had around 65,000 files related to it stolen by the Play ransomware gang during an attack on an IT supplier

The Week in Ransomware - March 8th 2024 - Waiting for the BlackCat rebrand
BleepingComputer.com - March 8 2024

We saw another ransomware operation shut down this week after first getting breached by law enforcement and then targeting critical infrastructure, putting them further in the spotlight of the US government.