Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

20 March 2024

Vulnerabilities

TeamCity Vulnerability Exploits Lead to Jasmin Ransomware, Other Malware Types

Trend Micro Simply Security - RSS - March 20 2024

CVE-2024-27198 and CVE-2024-27199 are vulnerabilities within the TeamCity On-Premises platform that can allow attackers to gain administrative control over affected systems.

SQL Injection Vulnerability Patched in Tutor LMS WordPress Plugin

Wordfence - RSS - March 19 2024

On February 15th, 2024, during our second Bug Bounty Extravaganza, we received a submission for an authenticated SQL Injection vulnerability in Tutor LMS, a WordPress plugin with more than 80,000+ active installations. This vulnerability can be leveraged to extract sensitive data from the database, such as password hashes...

Franklin Fueling System EVO 550/5000

CISA Current Activity - March 19 2024

Vendor: Franklin Fueling System Equipment: EVO 550, EVO 5000 Vulnerability: Path Traversal 2. RISK EVALUATION Successful exploitation of this vulnerability could allow an attacker to read arbitrary files on the system.

Malware and threat actors

Unit 42 Collaborative Research With Ukraine's Cyber Agency To Uncover the Smoke Loader Backdoor

Unit 42 – Palo Alto Networks Blog - March 19 2024

A surge in use of malware Smoke Loader by threat group UAC-0006 is highlighted in the first-ever joint research published by Unit 42 and SSSCIP Ukraine. The post Unit 42 Collaborative Research With Ukraine's Cyber Agency To Uncover the Smoke Loader Backdoor appeared first on Unit 42.

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

[CISA and Partners Release Joint Fact Sheet for Leaders on PRC-sponsored Volt Typhoon Cyber Activity]

CISA Current Activity - March 19 2024

Today, CISA, the National Security Agency (NSA), Federal Bureau of Investigation (FBI), and other U.S. and international partners are issuing a joint fact sheet, People's Republic of China State-Sponsored Cyber Activity:

Suspected Russian Data-Wiping 'AcidPour' Malware Targeting Linux x86 Devices

MalwareTips.com - March 19 2024

A new variant of a data wiping malware called AcidRain has been detected in the wild that's specifically designed for targeting Linux x86 devices.The malware, dubbed AcidPour, is compiled for Linux x86 devices, SentinelOne's Juan Andres Guerrero-Saade said in a series of posts on X... Click to expand...
Read more