Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

22 March 2024

Vulnerabilities

CVE-2023-48788: Fortinet FortiClientEMS SQL Injection Deep Dive

Security Boulevard - RSS - March 21 2024

Introduction In a recent PSIRT, Fortinet acknowledged CVE-2023-48788 – a SQL injection in FortiClient EMS that can lead to remote code execution. FortiClient EMS is an endpoint management solution for enterprises that provides a central location for...

CISA Releases One Industrial Control Systems Advisory

CISA Current Activity - March 21 2024

CISA released one Industrial Control Systems (ICS) advisory on March 21, 2024. These advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS. ICSA-24-081-01 Advantech WebAccess/SCADA CISA encourages users and administrators to review the newly released ICS advisory for technical details and mitigations.

CVE-2024-27438: Apache Doris: Downloading arbitrary remote jar files resulting in remote command execution

Open Source Security - March 21 2024

Download of Code Without Integrity Check vulnerability in Apache Doris. The jdbc driver files used for JDBC catalog is not checked and may resulting in remote command execution. Once the attacker is authorized to create a JDBC catalog, he/she can use arbitrary driver jar file with unchecked code
snippet.

Malware and threat actors

Mounting AceCryptor malware attacks target Europe

SC Magazine US - March 21 2024

TLP CLEAR: Disclosure is not limited

Organizations across Europe have been subjected to a deluge of attacks involving AceCryptor malware as part of campaigns that sought to exfiltrate email and browser credentials during the second half of 2023, reports The Record, a news site by cybersecurity firm Recorded Future. I

Ransomware Group "RA World" Changes Its' Name and Begins Targeting Countries Around the Globe

KnowBe4 - Blog - RSS - March 21 2024

The threat group "RA World" (formerly RA Group) has shifted from country-specific ransomware attacks to include specific industries via a new - not previously seen - method of extortion.

The Magnet Goblin group is leveraging one-day vulnerabilities

Security Magazine - March 21 2024

Recent research has shown that Magnet Goblin, a financially motivated threat actor group, exploits one-day vulnerabilities as a preliminary infection vector. The group predominantly targets public-facing servers and deploys Nerbian malware, such as...

Guidance

CISA, FBI, and MS-ISAC Release Update to Joint Guidance on Distributed Denial-of-Service Techniques

CISA Current Activity - March 21 2024

Today, CISA, the Federal Bureau of Investigation (FBI), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) released an updated joint guide, Understanding and Responding to Distributed Denial-Of-Service Attacks, to address the specific needs and challenges faced by organizations in defending against DDoS attacks. The guidance now includes detailed insight into three different types of DDoS techniques: Volumetric, attacks aiming to consume available bandwidth. Protocol, attacks which exploit vulnerabilities in network protocols. Application, attacks targeting vulnerabilities in specific applications or running services.

Windows 10 has a built-in ransomware block, you just need to enable it

MalwareTips.com - March 21 2024

Found these articles surprising, I was aware of Controlled folder access for years and it seems many windows users were not. Since the Windows OS has the highest amount of

TLP CLEAR: Disclosure is not limited

Ransomware attacks globally it maybe a good idea to have this protection feature enabled.