Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

13 March 2024

Vulnerabilities

'Magnet Goblin' Exploits Ivanti 1-Day Bug in Mere Hours
Dark Reading - March 12 2024

A prolific but previously hidden threat actor turns public vulnerabilities into working exploits before companies have time to patch.

CVE-2024-27135: Apache Pulsar: Improper Input Validation in Pulsar Function Worker allows Remote Code Execution
Open Source Security - March 12 2024

Improper input validation in the Pulsar Function Worker allows a malicious authenticated user to execute arbitrary Java code on the Pulsar Function worker.

Schneider Electric EcoStruxure Power Design
CISA Current Activity - March 12 2024

Vendor: Schneider Electric Equipment: EcoStruxure Power Design Vulnerability: Deserialization of Untrusted Data. Successful exploitation of this vulnerability may allow for arbitrary code execution.

Microsoft Releases Security Updates for Multiple Products
CISA Current Activity - March 12 2024

Microsoft has released security updates to address vulnerabilities in multiple products.

Hackers leverage 1-day vulnerabilities to deliver custom Linux malware
Help Net Security - News - March 12 2024

A financially motivated threat actor is using known vulnerabilities to target public-facing services and deliver custom malware to unpatched Windows and Linux systems. Among the exploited vulnerabilities are also two recently discovered Ivanti Connect Secure VPN flaws that are widely exploited by a variety of attackers.

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Malware and threat actors

Stanford: Data of 27,000 people stolen in September ransomware attack
BleepingComputer.com - March 12 2024

Stanford University says the personal information of 27,000 individuals was stolen in a ransomware attack impacting its Department of Public Safety (SUDPS) network.

BianLian ransomware crew exploiting bugs in JetBrains' TeamCity platform
SC Magazine US - March 12 2024

The BianLian ransomware gang is exploiting known bugs in JetBrains' TeamCity software development platform to gain initial access to victims' systems.

Anatomy of a BlackCat Attack
Red Sky Alliance - X-Industry - RSS - March 12 2024

A company contacted the incident response firm Sygnia to investigate suspect activity on its network.

Alert: FBI Warns Of BlackCat Ransomware Healthcare Attack
Tech-Wreck InfoSec Blog - March 12 2024

In recent months, a concerning trend has emerged within the healthcare sector: the resurgence of BlackCat ransomware attacks. The BlackCat ransomware healthcare attack has prompted a joint advisory from the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Department of Health and Human Services (HHS) warning healthcare organizations,