Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

13 February 2024

Vulnerabilities

CISA Adds One Known Exploited Vulnerability to Catalog
CISA Current Activity - February 12 2024

CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. CVE-2023-43770 Roundcube Webmail Persistent Cross-Site Scripting (XSS) Vulnerability These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise. Binding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities established the Known Exploited

Critical Vulnerability in Shim Impacts Major Linux Distributors (CVE-2023-40547)
Qualys Threat Protection - February 12 2024

Shim is a crucial software most Linux distributions use in the boot process to support Secure Boot. At the start of the month, Bill Demirkapi of the Microsoft Security Response Center (MSRC) discovered a critical severity vulnerability.

Malware and threat actors

Researchers released a free decryption tool for the Rhysida Ransomware
Security Affairs - February 12 2024

Researchers discovered a vulnerability in the code of the Rhysida ransomware that allowed them to develop a decryption tool. Cybersecurity researchers from Kookmin University and the Korea Internet and Security Agency (KISA) discovered an implementation vulnerability in the source code of the Rhysida ransomware. The experts exploited the vulnerability to reconstruct encryption keys and developed a decryptor that allows victims of the Rhysida ransomware to recover their encrypted data for free.

LockBit Ransomware Rampage: 10 Alleged Victims Fall to Cyber Siege!
The Cyber Express - February 12 2024

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

The notorious LockBit ransomware group has recently struck again, allegedly targeting a diverse range of entities and adding ten new victims to their dark web portal. Among the victims of this latest LockBit cyberattack are Silver Airways, Taiwan Textiles.

US Dismantles Warzone RAT Malware Operation
Infosecurity Today - February 12 2024

US authorities have seized domains and arrested individuals in connection with the Warzone RAT

Dark Storm Team Announces Cyberattack Targeting NATO, Israel, and Allies.
The Cyber Express - February 12 2024

The hacking group Dark Storm Team has issued a menacing ultimatum, vowing to unleash a wave of cyberattacks targeting the services and government websites of NATO countries , Israel, and those nations lending support to the Israeli cause.

Data breach of two third-party payment operators affects more than 33 million in France: CNIL opens an investigation
DataBreaches.net - February 12 2024

Google translation of some of CNIL's report: The CNIL was informed by Viamedis and Almerys of the computer attack to which they were victims.