Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

14 February 2024

Vulnerabilities

DarkMe Malware Targets Traders Using Microsoft SmartScreen Zero-Day Vulnerability

The Hacker News - February 14 2024

A newly disclosed security flaw in the Microsoft Defender SmartScreen has been exploited as a zero-day by an advanced persistent threat actor called Water Hydra (aka DarkCasino) targeting financial market traders. Trend Micro, which began tracking the campaign in late December 2023, said it entails the exploitation of CVE-2024-21412.

Attackers target new Ivanti XXE vulnerability days after patch

CSO Magazine - February 13 2024

Days after Ivanti announced patches for a new vulnerability in its Connect Secure and Policy Secure products, proof-of-concept exploit code has already been published for the flaw and security companies are reporting exploitation attempts in the wild. This follows a difficult month for Ivanti customers who had to deploy emergency mitigations and patches for three different zero-day vulnerabilities that were being exploited in the wild.

Adobe Releases Security Updates for Multiple Products

CISA Current Activity - February 13 2024

Adobe has released security updates to address vulnerabilities in Adobe software. A cyber threat actor could exploit some of these vulnerabilities to take control of an affected system. CISA encourages users and administrators to review the following Adobe Security Bulletins and apply the necessary updates.

CISA Releases One Industrial Control Systems Advisory

CISA Current Activity - February 13 2024

CISA released one Industrial Control Systems (ICS) advisory on February 13, 2024. ICSA-24-044-01 Mitsubishi Electric MELSEC iQ-R Series Safety CPU - CISA encourages users and administrators to review the newly released ICS advisory for technical details and mitigations.

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

[Microsoft February 2024 Patch Tuesday fixes 2 zero-days, 74 flaws]
BleepingComputer.com - February 13 2024

Today is Microsoft's February 2024 Patch Tuesday, which includes security updates for 74 flaws and two actively exploited zero-days. [...]

[Roundcube webmail XSS vulnerability exploited by attackers (CVE-2023-43770)]
Help Net Security - February 13 2024

CVE-2023-43770, a vulnerability in the Roundcube webmail software that has been fixed in September 2023, is being exploited by attackers in the wild, CISA has warned by adding the vulnerability to its Known Exploited Vulnerabilities (KEV) catalog.

Malware and threat actors

[Midnight Blizzard and Cloudflare-Atlassian Cybersecurity Incidents: What to Know]
The Hacker News - February 13 2024

The Midnight Blizzard and Cloudflare-Atlassian cybersecurity incidents raised alarms about the vulnerabilities inherent in major SaaS platforms. These incidents illustrate the stakes involved in SaaS breaches — safeguarding the integrity of SaaS apps and their sensitive data is critical but is not easy.

[Kasseika Ransomware Deploys BYOVD Attacks, Abuses PsExec and Exploits Martini Driver]
Trend Micro Research News Perspectives - February 14 2024

In this blog, we detail our investigation of the Kasseika ransomware and the indicators we found suggesting that the actors behind it have acquired access to the source code of the notorious BlackMatter ransomware.