Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

10 January 2023

Vulnerabilities

Microsoft starts off new year with relatively light Patch Tuesday, no zero-days

Talos Intelligence Blog - January 9 2024

Microsoft followed up one of the lightest recent Patch Tuesdays in December with another month of no zero-day vulnerabilities and only two critical issues. Many of the company's monthly security updates in 2023 included vulnerabilities that were actively being exploited in the wild or had publicly available exploits already in circulation. The company started out 2024 by disclosing 48 vulnerabilities on Tuesday across its suite of products and services, 46 of which are considered of "important" severity. One of the critical vulnerabilities patched Tuesday is CVE-2024-20674, a security bypass vulnerability in the Windows Kerberos authentication protocol.

High-severity RCE among 6 bugs added to CISA's exploited vulnerability catalog

SC Magazine US - January 9 2024

The Cybersecurity and Infrastructure Security Agency (CISA) on Monday added six new bugs to its Known Exploited Vulnerabilities (KEV) catalog. While the vulnerabilities included flaws in Cold Fusion, D-Link, Joomla!, and Apache products, arguably the most notable was CVE-2023-41990, a high-severity remote code execution (RCE) vulnerability in the Apple-only ADJUST TrueType font instruction, a bug that was at the center of setting off what is known as the "Operation Triangulation" attacks.

CISA Releases One Industrial Control Systems Advisory

CISA Current Activity - January 9 2024

CISA released one Industrial Control Systems (ICS) advisory on January 9, 2024. These advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS. ICSA-23-348-01 Cambium ePMP 5GHz Force 300-25 Radio (Update A) CISA encourages users and administrators to review the newly released ICS advisories for technical details and mitigations.

Fortinet Releases Security Updates for FortiOS and FortiProxy

CISA Current Activity - January 9 2024

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Fortinet has released a security update to address a vulnerability in FortiOS and FortiProxy software. A cyber threat actor could exploit this vulnerability to take control of an affected system. CISA encourages users and administrators to review the FG-IR-23-315 FortiOS & FortiProxy - Improper authorization for HA requests security bulletin and apply necessary updates.

Path Traversal Bug Besets Popular Kyocera Office Printers
Dark Reading - January 9 2024

A newly published path traversal vulnerability could enable account takeover, data theft, and follow-on attacks at organizations using Kyocera printers and other multifunction devices. Kyocera is a Japanese electronics manufacturer known for its multifunction printers.

Ransomware

Hackers target Microsoft SQL servers in Mimic ransomware attacks
Bleeping Computer - January 9 2024

A group of financially motivated Turkish hackers targets Microsoft SQL (MSSQL) servers worldwide to encrypt the victims' files with Mimic (N3ww4v3) ransomware. These ongoing attacks are tracked as RE#TURGENCE and have been directed at targets in the European Union, the United States, and Latin America.

Ransomware Attackers Add Swatting to their Arsenal of Threats
Bitdefender - January 9 2024

Ransomware attackers have expanded their blackmail toolbox and no longer rely solely on blocking critical systems and threatening to release stolen data. Some attackers are now resorting to swatting threats against victims, adding yet another threat to the menace of ransomware.

ProxyShell-targeting Babuk Tortilla ransomware decrypted after hacker’s arrest
SC Media - January 9 2024

A free decryptor is available to recover files affected by Babuk malware variant targeting Microsoft Exchange.

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Malware and threat actors

North Korea’s Lazarus Group Moved More Than $1 Million in BTC After Period of Dormancy

Bitdefender - January 9 2024

The infamous North Korean state-sponsored Lazarus Group suddenly transferred over $1 million worth of Bitcoin from a crypto mixer to an inactive wallet after a few weeks of radio silence. The perpetrators moved 27,371 BTC, worth approximately $1.2 million, in two transactions, said blockchain analysis company Arkham Intelligence, which spotted the transaction.

Blackjack hackers target Moscow ISP in retaliation for Kyivstar cyberattack

SiliconANGLE - January 9 2024

Pro-Ukrainian hacking group Blackjack has claimed to have breached a Moscow internet service provider in revenge for a Russian attack last month on Kyivstar, Ukraine's largest telecom provider. The cyberattack targeted Moscow-based M9 Telecom and is reported to have destroyed the provider's servers, deleting about 20 terabytes of data.