Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

24 January 2024

Vulnerabilities

Watch out, a new critical flaw affects Fortra GoAnywhere MFT

Security Affairs - January 23 2024

Fortra addressed a new authentication bypass vulnerability impacting GoAnywhere MFT (Managed File Transfer) product. Fortra warns customers of a new authentication bypass vulnerability tracked as CVE-2024-0204 (CVSS score 9.8), impacting the GoAnywhere MFT (Managed File Transfer) product.

Evernote Remote Code Execution Vulnerability (CVE-2023-50643)

Qualys Threat Protection - January 23 2024

Evernote is vulnerable to a flaw that can lead to remote code execution on successful exploitation. Tracked as CVE-2023-50643, the vulnerability has a critical severity rating and a CVSS score of 9.8.

CISA Releases Six Industrial Control Systems Advisories

CISA Current Activity - January 23 2024

CISA released six Industrial Control Systems (ICS) advisories on January 23, 2024. These advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS. ICSA-24-023-01 APsystems Energy Communication Unit (ECU-C) Power Control Software ICSA-24-023-02 Crestron AM-300 ICSA-24-023-03 Voltronic Power ViewPower Pro ICSA-23-023-04 Westermo Lynx 206-F2G ICSA-24-023-05 Lantronix XPort ICSMA-24-023-01 Orthanc Osimis DICOM Web Viewer CISA encourages users and administrators to review the newly released ICS advisories for technical details and mitigations.

UK cyber

Black Basta gang claims the hack of the UK water utility Southern Water

Security Affairs - January 23 2024

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

The Black Basta ransomware gang claimed to have hacked the UK water utility Southern Water, a major player in the UK water industry. Southern Water is a private utility company responsible for collecting and treating wastewater in Hampshire, the Isle of Wight, West Sussex, East Sussex and Kent, and for providing public water supply to approximately half of this area.

Ransomware

Subway Puts a LockBit Investigation on the Menu
Dark Reading - January 23 2024

The foot-long sandwich purveyor is looking into LockBit 3.0 claims that it stole reams of data from the proprietary "SBS" network.

Malware and threat actors

FBI and CISA Warn of Androxgh0st Malware Attacks
Security Bloggers Network - January 23 2024

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) have issued a joint Cybersecurity Advisory warning of the escalating threat posed by Androxgh0st malware. Threat actors are using this Python-scripted malware to build a botnet focused on cloud credential theft, with the stolen information being leveraged to deliver additional malicious payloads.

Dark Web Profile: INC Ransom
SOCRadar - January 24 2024

The digital world is constantly under the threat of cyber attacks, and the emergence of new ransomware groups only intensifies this peril. One such group that has recently come into the spotlight is INC Ransom.

Monthly Threat Actor Group Intelligence Report, November 2023 (ENG)
NSHC Red Alert - January 23 2024

This report is a summary of Threat Actor group activities analyzed by the NSHC ThreatRecon team based on data and information collected from 21 October 2023 to 20 November 2023.