Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

28 February 2024

Vulnerabilities

Black Basta and Bl00dy ransomware gangs exploit recent ConnectWise ScreenConnect bugs

Security Affairs - February 27 2024

New threat actors have started exploiting ConnectWise ScreenConnect vulnerabilities, including the Black Basta and Bl00dy ransomware gangs. Multiple threat actors have started exploiting the recently disclosed vulnerabilities, tracked as CVE-2024-1709 (CVSS score of 10) and CVE-2024-1708 (CVSS score of 8.4), in the ConnectWise ScreenConnect software.

Malware and threat actors

FBI, CISA warn US hospitals of targeted BlackCat ransomware attacks

Bleeping Computer - February 27 2024

Today, the FBI, CISA, and the Department of Health and Human Services (HHS) warned U.S. healthcare organizations of targeted ALPHV/Blackcat ransomware attacks. "ALPHV Blackcat affiliates have been observed primarily targeting the healthcare sector," the joint advisory cautions.

Russian hackers hijack Ubiquiti routers to launch stealthy attacks

Bleeping Computer - February 27 2024

Russian military hackers are using compromised Ubiquiti EdgeRouters to evade detection, the FBI says in a joint advisory issued with the NSA, the U.S. Cyber Command, and international partners.

New APT29 attacks set sights on cloud services

SC Magazine US - February 27 2024

Cyberespionage operations by Russian threat operation APT29, also known as Cozy Bear, The Dukes, and Midnight Blizzard, were noted by the Five Eyes intelligence alliance to be pivoting toward intrusions against cloud infrastructure, according to BleepingComputer.

Santesoft Sante DICOM Viewer Pro

CISA Current Activity - February 27 2024

Vendor: Santesoft Equipment: Sante DICOM Viewer Pro Vulnerability: Out-of-Bounds Read. Successful exploitation of this vulnerability could allow an attacker to disclose information and execute arbitrary code on affected installations of the product.

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

German state of Hessen says systems encrypted by ransomware

Bleeping Computer - February 27 2024

The German state of Hessen (Hesse) has been hit with a ransomware attack, causing the government to shut down IT systems and disrupting the availability of its consumer advice center.

Mitsubishi Electric Multiple Factory Automation Products

CISA Current Activity - February 27 2024

Vendor: Mitsubishi Electric Corporation Equipment: MELSEC iQ-F Series Vulnerability. Successful exploitation of this vulnerability could allow a remote attacker to cause a temporary denial-of-service (DoS) condition for a certain period of time in the product's Ethernet communication by performing a TCP SYN Flood attack.