Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

27 February 2024

Vulnerabilities

WordPress Plugin Alert - Critical SQLi Vulnerability Threatens 200K+ Websites
The Hacker News - February 27 2024

A critical security flaw has been disclosed in a popular WordPress plugin called Ultimate Member that has more than 200,000 active installations. The vulnerability, tracked as CVE-2024-1071, carries a CVSS score of 9.8 out of a maximum of 10.

ScreenConnect flaws exploited to deliver all kinds of malware (CVE-2024-1709, CVE-2024-1708)
Help Net Security - February 26 2024

The recently patched vulnerabilities (CVE-2024-1709, CVE-2024-1708) in ConnectWise ScreenConnect software are being exploited by numerous attackers to deliver a variety of malicious payloads.

Malware and threat actors

LoanDepot Ransomware Attack Leads to Data Breach; 17 Million Impacted
HackRead - February 26 2024

LoanDepot identified the ransomware attack on January 4, 2024.

UnitedHealth subsidiary Optum hack linked to BlackCat ransomware
Bleeping Computer - February 27 2024

A cyberattack on UnitedHealth Group subsidiary Optum that led to an ongoing outage impacting the Change Healthcare payment exchange platform was linked to the BlackCat ransomware group by sources familiar with the investigation.

ALPHV/BlackCat responsible for Change Healthcare cyberattack
The Register - Security - RSS - February 26 2024

The ALPHV/BlackCat ransomware gang is reportedly responsible for the massive Change Healthcare cyberattack that has disrupted pharmacies across the US.

The UK has seen an increase in cyberattacks against higher education
Security Magazine - February 26 2024

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

A report by KnowBe4 revealed that there has been an increase in cyberattacks against the UK's higher education institutions. Universities in the UK are common targets for cyberattackers, as they are typically associated with research facilities.

New IDAT Loader Attacks Using Steganography to Deploy Remcos RAT
The Hacker News - February 26 2024

Ukrainian entities based in Finland have been targeted as part of a malicious campaign distributing a commercial remote access trojan known as Remcos RAT using a malware loader called IDAT Loader.

Pikabot returns with new tricks up its sleeve
Help Net Security - News - February 26 2024

After a short hiatus, Pikabot is back, with significant updates to its capabilities and components and a new delivery campaign. About the Pikabot loader Pikabot is a loader – a type of malware whose primary function is to serve as a delivery mechanism for other malware.

CISA, NCSC-UK, and Partners Release Advisory on Russian SVR Actors Targeting Cloud Infrastructure
CISA Current Activity - February 26 2024

CISA, in partnership with UK National Cyber Security Centre (NCSC) and other U.S. and international partners released the joint advisory, SVR Cyber Actors Adapt Tactics for Initial Cloud Access.

IntelBroker claimed the hack of the Los Angeles International Airport
Security Affairs - February 26 2024

The popular hacker IntelBroker announced that it had hacked the Los Angeles International Airport by exploiting a flaw in one of its CRM systems. The website Hackread first reported that the popular hacker IntelBroker had breached one of the CRM systems used by the Los Angeles International Airport.