WEEKLY BULLETIN
16-20 OCTOBER 2023

Quote

"If security were all that mattered, computers would never be turned on, let alone hooked into a network with literally millions of potential intruders.".

Dan Farmer

of the week

Content:

- **Cyber Security in Healthcare Sector**

- **Security advice for the healthcare sector**

Cyber Security in Healthcare Sector

"Hospital's systems were already fragile before the pandemic. Then ransomware attacks became more varied, more aggressive and with higher payment demands."

Josh Corman

Healthcare cybersecurity is a strategic imperative for any organization in the medical industry — from healthcare providers to insurers to pharmaceutical, biotechnology and medical device companies.

It involves a variety of measures to protect organizations from external and internal cyber attacks and ensure availability of medical services, proper operation of medical systems and equipment, preservation of confidentiality and integrity of patient data, and compliance with industry regulations.

Security advice for the healthcare sector

Prevent unauthorized access

Use multi-factor authentication which ensures that only authorized users can access confidential data.

Strengthen network security

Firewalls are vital components of network security. Firewalls block unauthorized access to a network. On the other hand, intrusion detection systems detect and react to potential cyber threats.

Perform regular software updates

Regular system updates are effective measures against known vulnerabilities. They reduce the risk of cyber-attacks and introduce the most powerful security solutions to date.

WEEKLY BULLETIN
16–20 OCTOBER 2023

Content:

- **FBI and CISA warn of ransomware attacks on critical infrastructure sectors**

- **42,000 Cisco IOS XE devices actively exploited**

- **Discord: A Playground for Nation-State Hackers Targeting Critical Infrastructure**

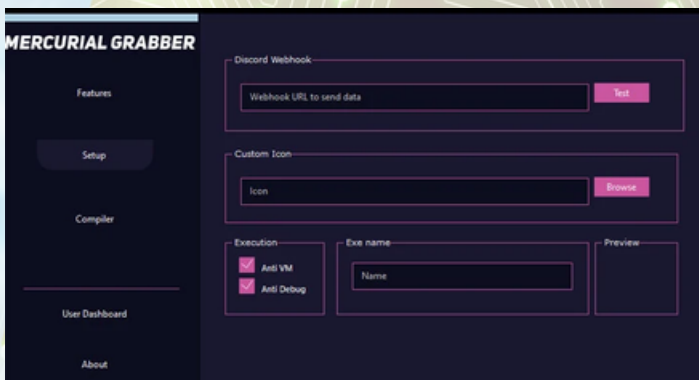- **Oracle - patching alert**

YOUR FILES ARE ENCRYPTED

FBI and CISA warn of ransomware attacks on critical infrastructure sectors

A new joint cybersecurity advisory published by CISA and the FBI as part of the #StopRansomware project shares the indicators, tactics, techniques and procedures (TTP) of the AvosLocker ransomware-as-a-service (RaaS) operation.

CISA and the FBI recommend that organizations implement the necessary mitigation measures to reduce the impact of AvosLocker ransomware and other ransomware incidents.

Read more

42,000 Cisco IOS XE devices actively exploited

Security researchers have found thousands of exploited hosts linked to a critical zero-day vulnerability in the web user interface of Cisco IOS XE software.

Cisco announced that the company is working to develop a patch, however warned that there is no existing solution. The company urges users to disable the HTTP Server feature on their systems.

Read more

MERCURIAL GRABBER

Discord: A Playground for Nation-State Hackers Targeting Critical Infrastructure

According to a new report from Trellix researchers, the Discord platform, one of the most widely used communication applications worldwide, is increasingly being abused by attackers who use its infrastructure to carry out their operations.

The way a malware attack abuses Discord focuses on two main techniques: downloading additional files and extracting information.

Among the most popular malware observed to have targeted Discord are Mercurial Grabber, Stealerium, Typhon Stealer, and Venom RAT.

Read more

PATCHING ALERT

ORACLE Critical Patch Update

Oracle - patching alert

Oracle has released 387 new security patches that address 185 vulnerabilities in its code and third-party components.

More than 40 security patches address vulnerabilities rated as critical and more than 200 resolve vulnerabilities that can be exploited remotely.

NAECCS advises all Oracle users to perform the necessary updates.

Read more