12 Aug 22

Cyber Threat Roundup

A collection of recent open-source items of interest to the Defense Industrial Base

Contents

Articles

FBI: Zeppelin Ransomware May Encrypt Devices Multiple Times in Attacks

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) warned U.S. organizations today that attackers deploying Zeppelin ransomware might encrypt their files multiple times. The FBI also asked IT admins who detect Zeppelin ransomware activity within their enterprise networks to collect and share any related information with their local FBI Field Office.

https://www.bleepingcomputer.com/news/security/fbi-zeppelin-ransomware-may-encrypt-devices-multiple-times-in-attacks/

Cisco Releases Advisories for Bug Affecting More Than One Million Security Devices

Cisco on Thursday released three advisories for vulnerabilities discovered by cybersecurity firm Rapid7 in its Adaptive Security Software (ASA) and ASA-X systems. More than one million Cisco ASA devices are deployed worldwide and are designed to support VPN, IPS, and many other features.

https://therecord.media/cisco-releases-advisories-for-bug-affecting-more-than-1-million-security-devices/

Cisco Confirms Data Breach, Hacked Files Leaked

An attacker compromised a Cisco employee's personal Google account, which gave them access to the worker's business credentials through the synchronized password store in Google Chrome. Eventually, the worker, either inadvertently or through alert fatigue, accepted the push request, giving the attacker access to Cisco's network.

https://www.darkreading.com/attacks-breaches/cisco-confirms-data-breach-hacked-files-leaked

Three Ransomware Attacks Hit Single Company Over Two Weeks

Three of the most prolific ransomware gangs currently in operation targeted the same company over a period of two weeks, according to cyber security researchers. An unidentified automotive company was the victim of three separate ransomware attacks at the hands of LockBit, Hive, and AlphV – the latter sometimes referred to as "BlackCat" – almost simultaneously.

https://www.itpro.co.uk/security/ransomware/368795/three-ransomware-attacks-hit-single-company-over-two-weeks

Zimbra Auth Bypass Bug Exploited to Breach Over 1,000 Servers

An authentication bypass Zimbra security vulnerability is actively exploited to compromise Zimbra Collaboration Suite (ZCS) email servers worldwide. Successful exploitation allows the attackers to deploy web shells on specific locations on the compromised servers to gain persistent access.

https://www.bleepingcomputer.com/news/security/zimbra-auth-bypass-bug-exploited-to-breach-over-1-000-servers/

Onyx Ransomware Overwrites Files Over 2MB Instead of Encrypting Them

As early as mid-April of 2022, for the first time, researchers discovered Onyx ransomware. The ransomware group uses the double-extortion method of encrypting and exfiltrating data from a victim in order to extort money. The Onyx ransomware was created using the .NET architecture. After being executed successfully, this ransomware encrypts the files and drops a ransom note titled “readme.txt” containing the instructions for decrypting them.

https://cybersecuritynews.com/onyx-ransomware-overwrites-files-larger-than-2mb/