Health-ISAC™
Collaborating for Resilience in Healthcare

Daily Cyber Headlines

Daily Cyber Headlines ○ TLP:WHITE Alert ID : 07cfc82a Oct 23, 2024, 06:52 AM

Today's Headlines:

Leading Story

- VMware Fixes Critical vCenter Server RCE Bug – Again! (CVE-2024-38812)

Data Breaches & Data Leaks

- Radisson's Country Inn and Suites Allegedly Hit by Ransomware

Cyber Crimes & Incidents

- Cyprus Critical Infrastructure Targeted In Series of Cyberattacks, As Authorities Stress on Readiness
- IcePeony Hacker Exploiting Public Web Servers To Inject Webshells

Vulnerabilities & Exploits

- CISA Adds ScienceLogic SL1 Vulnerability To Exploited Catalog After Active Zero_Day Attack

Trends & Reports

- Latrodectus Malware Increasingly Used by Cybercriminals
- AI-Powered Attacks Flood Retail Websites

Privacy, Legal & Regulatory

- Nothing to Report

Upcoming Health-ISAC Events

- Global Monthly Threat Brief
    - Americas – October 29, 2024, 12:00-01:00 PM ET

  - European – October 30, 2024, 03:00-04:00 PM CET
- T-SIG Webinar for SMB Members – November 14, 2024 at 11:30 AM ET
- Fall Americas Summit, Phoenix, Arizona - December 2-6, 2024

Additional Information

Leading Story

VMware Fixes Critical vCenter Server RCE Bug – Again! (CVE-2024-38812)

Summary

- Broadcom releases another batch of updates for a pair of vulnerabilities affecting the vCenter Server.

Analysis & Action

Broadcom recently released updated patches for two previously disclosed vulnerabilities, CVE-2024-38812 and CVE-2024-38813, affecting vCenter Server. One of the two vulnerabilities was not fully addressed, and it can allow remote code execution on affected instances.

The vulnerability identified as CVE-2024-38812 is a security flaw in the DCERPC protocol that can allow threat actors to execute malware on affected vCenter Server instances by sending specially crafted network traffic. Conversely, CVE-2024-38813 allows threat actors to elevate privileges on vulnerable vCenter Server installations.

The newly released patches address the vulnerabilities and a session timeout issue when accessing vCenter. It is strongly recommended that users apply the new patches available here.

Data Breaches & Data Leaks

Radisson’s Country Inn and Suites Allegedly Hit by Ransomware

Summary

- Threat actor Everest's recent attack against the hotel chain exposed the personal information of thousands of clients.

Analysis & Action

A recent mid-level attack committed on the hotel chain containing Suites by Radisson & Country Inn discovered thousands of their client's personal information stolen. The hotel chain is a known subsidiary of Choice Hotels, which likely led to the compromise.

Amongst the data stolen through the cyberattacks were billing details, internal emails, credit card information, messages, incidents, and details from calendars of prior and upcoming bookings. Everest revealed the information in a post on Monday to their extortion site. The threat actor has also implemented a 10-day countdown and information for negotiations on their site. A more detailed investigation into the exposed data shows a compromise of reward account numbers for the chain, along with program billing and guest tax ID rewards. This comes after Radisson Hotels Americas had guest records compromised in the MOVEit campaign led by Cl0p. Everest, however, is believed to be associated with BlackByte, a ransomware-as-a-service group based in Russia.

With threat actors continuing to expand their attacks and associating with other threat actors to do so, the importance of protective strategies to protect sensitive information remains paramount. Health-ISAC recommends that its members use data backups and encryption methods to mitigate the risks of similar attacks.

Cyber Crimes & Incidents

Cyprus Critical Infrastructure Targeted in Series Of Cyberattacks, As Authorities Stress on Readiness

Summary

- Multiple facilities within Cyprus known for supporting critical infrastructure were targeted in a string of attacks that began Friday.

Analysis & Action

These attacks targeted various vital services, focusing on critical installations. Amongst the targets were the Bank of Cyprus, Telecommunications, Hermes Airport Website, and Cyprus Electricity Authority.

Though the attacks were confirmed to be legitimate, they were contained with quick action, and there was no disruption to any service. Several cyber threat actors had announced a plan to compromise Cypriot agencies weeks prior, including threat actor LulzSec Black. The cybersecurity firm of Cyprus, Odyssey, identified the attack and the potential tactics the threat actor intended to use. Potential tactics the firm identified were mainly data breaches and distributed denial of service (DDoS) attacks, aiding the country in protecting itself against the upcoming attacks. A Monday report claimed the country had experienced a series of major attacks. However, the attacks targeted internet infrastructure and government websites, private businesses, and public services saw impacts of these attacks. Additionally, The Bank of Cyprus was then targeted, and then Saturday saw Telecommunications targeted. These attacks were likely distributed by multiple threat actors as groups such as Moroccan Soldiers, Anonymous Syria, and Black Maskers Army are amongst those with intent to attack Cyprus infrastructure as well.

Health-ISAC recommends its members remove all unnecessary services or legacy systems from their devices to mitigate entry risks exploiting weak points. Additionally, including MFA tools can help act against threat actors who intend to breach data.

IcePeony Hacker Exploiting Public Web Servers To Inject Webshells

Summary

- Threat actor IcePeony utilizes ISS malware IceCache, exploiting injection vulnerabilities within SQL.

Analysis & Action

The threat actor IcePeony is fairly new, with their activity only spanning from 2023. They are known to target countries like Mauritius, India, and Vietnam.

The threat actor's main method of attack is exploitation regarding injection vulnerabilities in SQL. With this, they can compromise systems via the use of backdoors and webshells with their customized malware called IceCache. However, the threat actor recently exposed sensitive data pertaining to them by accident, this data revealed their techniques and timeline of attacks. Amongst the revealed tools lies a tool named Stax, a version of Stowaway that encrypts communication targets with AES and Base64 for network and security traffic. In addition, the threat actor used ProxyChains, executing scripts linux_back.sh and info.sh to their victims to gain their information and deploy their rootkit named Diamorphine. The IceCache malware is designed for intrusion, offering several capabilities like file transfers, command execution, and proxy services. Though the threat actor's specific location is unknown at this time, it was also identified that they operate under the UTC +8 time zone and are believed to be state-sponsored in China.

As this fairly new threat actor continues to improve their capabilities over time, it remains important to bolster protection against these types of malware attacks. Health-ISAC recommends its members utilize trusted intrusion prevention systems (IPS) to block attack methods.

Vulnerabilities & Exploits

CISA Adds ScienceLogic SL1 Vulnerability To Exploited Catalog After Active Zero-Day Attack

Summary

- After zero-day exploitation, the Cybersecurity and Infrastructure Security Agencies (CISA) Known Exploited Vulnerabilities (KEV) catalog added a critical security flaw.

Analysis & Action

The vulnerability concerns a bug within a third party that has not been publicly announced. This vulnerability could lead to remote code execution. It has since been tracked as CVE-2024-9537 and has received a CVSS v4 score of 9.3.

The vulnerability has been addressed within versions 12.1.3, 12.2.3, and 12.3 going forward. In addition, fixes have been made for version 10.1.x, 10.2.x, 11.1.x, 11.2.x, and 11.3.x. Rackspace, a multi-cloud technology service, became aware of the issue and went offline in response. At this time, Rackspace does not know who is responsible for the attacks, though the service company has confirmed methods of gaining unauthorized access to reporting systems internally. Additionally, CISA has added another vulnerability flaw to their KEV catalog, this time impacting Fortinet and its OS, PAM, Proxy, and Web services. The vulnerability was marked as CVE-2024-23113 and received a CVSS score of 9.8 due to its use of exploitation.

Threat actors continue to strengthen their attacks, finding new methods and vulnerabilities to exploit. Health-ISAC recommends that its members utilize trusted antivirus and malware software and firewalls to prevent similar attacks.

Trends & Reports

Latrodectus Malware Increasingly Used by Cybercriminals

Summary

- Threat actors are increasingly leveraging Latrodectus malware, targeting several industries.

Analysis & Action

The malware, initially assessed to have been developed by a threat actor associated with WizardSpider and the creator of IcedID, was detected in October 2023. Latrodectus malware is primarily spread through malicious attachments delivered via phishing emails in either PDF or HTML format.

When users interact with the attachments, malware is installed on their systems, leading to damages, including the exfiltration of personally identifiable information (PII), financial losses through fraud or extortion, and the compromise of other sensitive information.

The main difference between the PDF and HTML variants of the malware lies in the installation method. The PDF variant uses an MSI installer downloaded by JavaScript, while the HTML variant attempts to directly install a DLL using PowerShell. However, both leverage obfuscation techniques to hide the malicious JavaScript code embedded in the attachments.

Health-ISAC recommends that organizations remain vigilant to threat actors who deliver malware through sophisticated phishing campaigns to infiltrate networks and wreak havoc after executing a successful intrusion.

AI-Powered Attacks Flood Retail Websites

Summary

- Cybersecurity firm Imperva reveals that retailers experience over half a million AI-driven attacks per day.

Analysis & Action

According to a six-month analysis by Imperva, retailers have experienced over 569,884 AI-drive attacks per day. The AI tools being leveraged in these attacks include ChatGPT, Claude, and Gemini, as well as sophisticated bots to scrape websites for large language model (LLM) training data.

According to the analysis, the threat actors' operations included a range of AI-driven threats, including bots, distributed denial of service (DDoS) attacks, API violations, and business logic abuse. The security firm's research revealed that these threats account for the top AI-driven retail site attacks. Business logic abuse leads the way, accounting for 30.7% of all incidents, with DDoS attacks following at 30.6%, bad bots at 20.8%, and API violations at 16.1%.

It is important that organizations invest in robust cybersecurity measures to mitigate risks associated with threat actors' weaponization of AI. These measures include regularly updating security software, monitoring for suspicious activity, and implementing strong authentication methods.

Privacy, Legal & Regulatory

Nothing to Report.

Health-ISAC Cyber Threat Level

On October 17, 2024, the Health-ISAC Threat Intelligence Committee (TIC) evaluated the current Cyber Threat Level and collectively decided to raise the Cyber Threat Level to Yellow (Elevated). The Threat Level of Yellow (Elevated) is due to threats from:

The Threat Level of Yellow (Elevated) is due to threats from elections-related smishing campaigns, DPRK remote worker activity, potential repercussions of recent activity in the Middle East, commodity malware, and a recent uptick in ransomware events.

For more information about the Health-ISAC Cyber Threat Level, including definitions and response guidelines for each of the alert levels, please review the Threat Advisory System.

You must have Cyware Access to reach the Threat Advisory System document. Contact membership@h-isac.org for access to Cyware.

Report Source(s)

Health-ISAC

Reference | References

Infosecurity Magazine
The Hacker News
GB Hackers
Broadcom
Help Net Security
Security Week
industrialcyber
MSSP Alert

Tags

AI-Powered Attacks, Latrodectus Malware, ScienceLogic SL1 Vulnerability, IcePeony Hacker, Critical Infrastructure Attacks, Data Breaches, VMware

Share Threat Intel:

For guidance on sharing indicators with Health-ISAC via HTIP, please visit the Knowledge Base article "HTIP - Share Threat Intel" here.

The "Share Threat Intel" feature allows for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

Turn off Categories:

For guidance on disabling alert categories, please visit the Knowledge Base article "HTIP Alert Categories" here.

Access the Health-ISAC Threat Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments:

Please email us at toc@h-isac.org