Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : a06a4ce9 | Oct 11, 2024, 07:26 AM

Today's Headlines:

Leading Story

- The Global State of Internet of Healthcare Things (IoHT) Exposures on Public-Facing Networks

Data Breaches & Data Leaks

- The Wayback Machine Suffers Data Breach
- Russian Cyber Firm Dr.Web Denies Data Leak By Pro-Ukraine Hackers

Cyber Crimes & Incidents

- American Water Works Cybersecurity Incident: A Wake-Up Call For Critical Infrastructure

Vulnerabilities & Exploits

- Experts Warn of Critical Unpatched Vulnerability in Linear eMerge E3 Systems
- Multiple VMware NSX Vulnerabilities Let Attackers Gain Root Access

Trends & Reports

- Over 240 Million US Breach Victims Recorded in Q3

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
- European Summit, Athens, Greece - October 15-17, 2024
- Fall Americas Summit, Phoenix, Arizona - December 2-6, 2024

Health-ISAC will not be distributing Daily Cyber Headlines on Monday, October 14, due to the observance of the holiday Columbus/ Indigenous Peoples' Day.

Additional Information

Leading Story

The Global State of Internet of Healthcare Things (IoHT) Exposures on Public-Facing Networks

Summary

- Censys found 14,004 unique IP addresses exposing healthcare devices and data platforms, along with the sensitive data they store, to the public internet

Analysis & Action

Healthcare data breaches are increasing and are usually more costly than in other industries. Aside from the financial burden that breaches impose, breaches of healthcare specifically can also negatively affect human health and patient outcomes.

14,004 distinct IP addresses were discovered in a Censys investigation, exposing healthcare systems and equipment to the public internet and potentially sensitive medical data stored on them. Of all identified exposed hosts, 50% are in the US, followed by India at 10.5%. Open DICOM ports and DICOM-enabled web interfaces account for 36% of the exposures, while Electronic Medical Records (EMRs) and Electronic Health Records (EHRs) systems represent 28%.

Health-ISAC recommends minimizing the internet exposure of medical devices, establishing rigorous network access controls, and segmenting your network to minimize the risk of a successful attack that could result in a data breach.

Data Breaches & Data Leaks

The Wayback Machine Suffers Data Breach

Summary

- Threat actors breached the Internet Archive website, stealing a database containing information for 31 million user accounts.

Analysis & Action

This breach was confirmed on Wednesday after visitors encountered a hacker-created message displayed on the site.

The message, a mocking JavaScript alert, stated the Archive had suffered a catastrophic security breach. It also mentioned HIBP, referring to the Have I Been Pwned service, where compromised data is often uploaded.

Millions of these emails are already registered with HIBP and will soon be updated with the stolen data. Users can then check HIBP to see if their information was compromised.

Russian Cyber Firm Dr.Web Denies Data Leak By Pro-Ukraine Hackers

Summary

- Recent claims of DumpForums cyberattack have been denied by the Russian antivirus company Dr.Web

Analysis & Action

Pro-Ukraine group DumpForums recently claimed to have committed a breach on Dr.Web and stolen nearly ten terabytes of data. The antivirus company, however, came out Wednesday, denying the threat actor's claims.

The antivirus company said the claims were “mostly untrue” as user data was not affected, nor was any user at security risk from the attacks. This contradicts the claims made by the threat actor, stating they had access to the network and remained undetected for a month, breaching the company's GitLab server. The threat actors then provided links as proof of their successful attack. However, it is now unclear if those links validate the attacks. The company has come out to say that the attacks were stopped, and services were disconnected following security protocols in response to the threat actor. The company, at this time, claims to be unable to provide any more details as the

investigation is underway. Additionally, Dr.Web has failed to update malware and virus databases for numerous days following the cyber attack.

Data breaches and leaks are common tactics used by threat actors for their own monetary gain. As they continue to transpire, it is important to take proper precautions. Health-ISAC members should consider utilizing trusted encryption methods, structuring endpoint security, and monitoring network and third-party access.

Cyber Crimes & Incidents

American Water Works Cybersecurity Incident: A Wake-Up Call For Critical Infrastructure

Summary

- A recently reported cybersecurity breach highlights the risks of critical infrastructure security with cyberattacks.

Analysis & Action

One of the largest water utility companies in the U.S. faced a recent cybersecurity breach, exposing the vulnerabilities within its systems.

The company's findings uncovered that unauthorized activity was gained into its network, allowing the attack to occur. As a quick response to the activity, however, immediate action was taken to respond to the incident, disconnecting other systems as a precaution. Afterward, third-party cybersecurity services were contacted for further investigations into the breach. A larger trend is at play here as essential public services remain important for threat actors. The cyberattack had no substantial impact on the water services as the CISA began to monitor the sector to mitigate risks for future recurrences.

Health-ISAC members should consider remaining vigilant about their networks and systems and properly identifying any virtual vulnerabilities to mitigate the chances of similar attacks.

Vulnerabilities & Exploits

Experts Warn of Critical Unpatched Vulnerability in Linear eMerge E3 Systems.

Summary

- Cybersecurity experts have identified an unpatched critical security flaw in Nice Linear eMerge E3 access control systems.

Analysis & Action

The critical vulnerability, tracked as CVE-2024-9441, affects several versions of Nortek Linear eMerge E3 Access Control. Nortek Linear eMerge E3 is a series of access control systems for managing access to doors, gates, and other restricted areas.

Despite the vulnerability being disclosed late last month, the vendor has yet to provide a fix or a workaround. Due to the availability of proof-of-concept exploit code, risks of exploitation likely have increased as threat actors may attempt to take advantage of the unpatched solution.

Organizations should consider prioritizing mitigation strategies, including temporary restrictions, alternative solutions, or even decommissioning if the risk is deemed too high when faced with vulnerable products lacking vendor-provided fixes or workarounds.

Multiple VMware NSX Vulnerabilities Let Attackers Gain Root Access

Summary

- VMware discloses three vulnerabilities affecting VMware NSX and VMware Cloud Foundation.

Analysis & Action

VMware has identified three vulnerabilities in its NSX product line that allow attackers to gain root access.

The vulnerabilities, tracked as CVE-2024-38818, CVE-2024-38817, and CVE-2024-38815, have CVSS scores ranging from 4.3 to 6.7. They affect both VMware NSX and VMware Cloud Foundation. The vulnerabilities include command injection, local privilege escalation, and content spoofing.

Health-ISAC advises organizations with vulnerable VMware instances to immediately update to fixed software versions to mitigate the risk of exploitation.

Trends & Reports

Over 240 Million US Breach Victims Recorded in Q3

Summary

- The 2024 Identity Theft Resource Center (ITRC) breach analysis report reveals significant data exposures despite not surpassing 2023's Q3 results.

Analysis & Action

Despite not surpassing data breach results tallied in Q3 of 2023, significant data exposures were observed in Q3 of 2024, citing a massive increase in supply chain attacks, according to a report by the Identity Theft Resource Center (ITRC).

The ITRC's latest quarterly report revealed a 77% decline in data breaches and leak victims. This is due to an inflation of numbers stemming from Q2's mega breaches at Ticketmaster and Advanced Auto Parts. As such, the total number of data compromises stands at 672 for Q3, reflecting an 8% quarterly decline.

One of the most notable points of the information disclosed in the recent report is that supply chain attacks have risen 203% quarter-on-quarter in Q3 after dropping in the first two quarters of 2024. The ITRC's report highlights significant trends in data breaches resulting from incidents that impacted numerous stakeholders. Therefore, it is critical that organizations prioritize data and identity protection.

Privacy, Legal & Regulatory

Nothing to Report.

Health-ISAC Cyber Threat Level

On September 19, 2024, the Health-ISAC Threat Intelligence Committee (TIC) evaluated the current Cyber Threat Level and collectively decided to maintain the Cyber Threat Level at Blue (Guarded). The Threat Level of Blue (Guarded) is due to threats from:

The Threat Level of Blue (Guarded) is due to threats from DPRK IT fraud, elections-induced cyber activity, potential repercussions of recent activity in the Middle East, potential Ivanti Endpoint Manager exploitation, and ongoing observances of infostealer's logs being posted on Telegram.

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

Incident Date

Oct 11, 2024, 05:59 PM

Reference | References

Medium
Censys
Infosecurity Magazine
Bleeping Computer
The Record
The Hacker News
GB Hackers

Tags

Breach Victims, VMware NSX Vulnerabilities, Linear eMerge E3 Systems Flaw, Internet of Healthcare Things (IoHT), Data Breaches

---

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