Health-ISAC™
SHARING SINCE 2010
Collaborating for Resilience in Healthcare

Daily Cyber Headlines

Daily Cyber Headlines ○ TLP:WHITE Alert ID : 08abdbf2 Oct 08, 2024, 07:59 AM

Today's Headlines:

Leading Story

- Health Sector Warned of New Trinity Ransomware Threats

Data Breaches & Data Leaks

- Personal Information Compromised in Universal Music Data

Cyber Crimes & Incidents

- Malware Attack On State Data Center In India Puts Some Citizen Services At A Standstill

Vulnerabilities & Exploits

- Critical Apache Avro SDK Flaw Allows Remote Code Execution In Java Applications
- Qualcomm Patches High-Severity Zero-Day Exploited in Attacks

Trends & Reports

- Ransomware Hits Critical Infrastructure Hard, Costs Adding Up

Privacy, Legal & Regulatory

- Fraud Repayment Rules Could Leave Victims Struggling, CTSI Claims

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 – October 10, 2024 at 11:30 AM ET
- European Summit, Athens, Greece - October 15-17, 2024
- Fall Americas Summit, Phoenix, Arizona - December 2-6, 2024

Additional Information

Leading Story

Health Sector Warned of New Trinity Ransomware Threats

Summary

- The healthcare sector has been warned about a new ransomware strain called Trinity, which opportunistically targets organizations across sectors.

Analysis & Action

The healthcare sector has been warned about a new ransomware strain called Trinity. The Trinity ransomware group has successfully compromised organizations across sectors, including healthcare, through phishing attacks, exploiting unpatched systems, and using stolen credentials.

After initial access, the group exfiltrates data and encrypts systems. After encryption, a ransom note is generated, with instructions and an email address. Victims have 24 hours to respond and pay a ransom in cryptocurrency or risk their data being leaked. The ransomware strain shares similarities with other ransomware groups, such as 2023Lock and Venus, suggesting a potential collaboration among threat actors.

Health-ISAC recommends members maintain a strong security posture by updating vulnerable devices timely, deploying anti-phishing security tools, and raising staff awareness about good security practices to minimize the risk of Trinity ransomware attacks. More information is available in Health-ISAC's alert here.

Data Breaches & Data Leaks

Personal Information Compromised in Universal Music Data Breach

Summary

- Universal Music Group informed several individuals that a recent data breach compromised personally identifiable information (PII).

Analysis & Action

According to Universal Music Group’s data breach notification to the Office of the Main Attorney General’s Office, the data breach occurred on July 15, 2024, and was discovered on August 30, 2024.

A total of 680 individuals were affected by the incident in which an unauthorized third party gained access to data that potentially included personal information, including names and Social Security numbers.

Notifications for those impacted by the data breach were disseminated on October 3, 2024, and consumers were provided with 24 months' worth of free credit monitoring and identity theft protection services. To prevent data breaches, Health-ISAC recommends implementing security measures that include strong access controls, encryption, regular security assessments, and employee training to safeguard sensitive information.

Cyber Crimes & Incidents

Malware Attack On State Data Center In India Puts Some Citizen Services At A Standstill

Summary

- Recently discovered malware at India's State Data Center has shut down their IT infrastructure, impacting multiple entities.

Analysis & Action

Friday, Uttarakhand was impacted after malware detection led to the closure of various services within the region. These services include the chief minister's helpline, government websites, and land registration services.

A cyberattack is behind the incident as recent investigations have been launched into the breach, discovering malware during a routine October 2 scanning. The suspicion of a cyberattack led to the closures to possibly weaken the possible damages that could have been incurred. As precautions continue to be taken, only 11 of the 1,378 virtual machines have been impacted by the malware, while no data loss has been reported. A cybersecurity task force has been called to act against the possible cyber attack as an additional means for security audits are being set up to avoid any future instances of similar veins.

Health-ISAC recommends utilizing trusted antivirus software and putting your network behind firewalls to mitigate your risks of possible cyber attacks distributing malware.

Vulnerabilities & Exploits

Critical Apache Avro SDK Flaw Allows Remote Code Execution In Java Applications

Summary

- Potential exploits to a critical security flaw (CVE-2024-47561) within Apache Avro impose risks on susceptible instances.

Analysis & Action

Apache Avro, a software development kit using Java, is now seeing a recent security flaw come to light with the potential for executing arbitrary code as a large risk of the flaw.

The flaw is being tracked as CVE-2024-47561, which impacts any software that has been present before 1.11.4. Due to this, recommendations have been released for individuals to upgrade their software to 1.11.4 or 1.12.0, zeroing the chances of the issue's impact. Research by the Avro team uncovered that the vulnerability will impact applications in which users are prompted to administer their own schema. The vulnerability can deserialize input from the schema, leading to the execution of the code. Various security implications exist as Apache Avro is an open-source project utilized by many organizations, and a patch for the vulnerability has yet to be released.

Health-ISAC recommends issuing the latest patches to software to mitigate risks. Additionally, checking information such as data types, objects, and record types can help act against similar acts of schema parsing by threat actors.

Qualcomm Patches High-Severity Zero-Day Exploited in Attacks

Summary

- Qualcomm patched multiple vulnerabilities, including a high-severity flaw being exploited in limited attacks.

Analysis & Action

Qualcomm has released security updates to address nearly two dozen flaws in its proprietary and open-source components, including one critical flaw and one high-severity flaw undergoing exploitation.

The high-severity vulnerability, CVE-2024-43047, is a user-after-free bug in the Digital Signal Processor Service that could lead to memory corruption. The flaw is currently undergoing exploitation, and while details are unknown to the public, it is suspected it might have been used in a spyware attack. The second important flaw included in the October updates is CVE-2024-33066. The flaw is caused by an improper input validation and could result in memory corruption. It has a CVSS score of 9.8, highlighting its criticality.

Health-ISAC recommends immediate patching of vulnerable devices as one of the most effective ways to improve security posture and minimize the risk of an attack.

Trends & Reports

Ransomware Hits Critical Infrastructure Hard, Costs Adding Up

Summary

- Ransomware attacks remain a serious threat to critical infrastructure entities, with healthcare being the most affected sector.

Analysis & Action

Ransomware attacks remain one of the biggest threats across industries, including critical infrastructure entities. Moreover, ransom demands and recovery efforts involve serious financial burdens.

The healthcare sector was the most affected, with 78% reporting ransom payments of more than $500,000. The need for remote access to CPS has increased organizations' exposure, resulting in a bigger attack surface. However, most respondents reported confidence in their organization's risk-reduction efforts.

To mitigate risks, organizations should build cybersecurity programs, perform risk assessments, secure remote access for third parties, improve network protections, and deploy threat detection capabilities.

Privacy, Legal & Regulatory

Fraud Repayment Rules Could Leave Victims Struggling, CTSI Claims

Summary

- Changes to rules regarding refunds for authorized push payment (APP) scams drastically reduced victim coverage.

Analysis & Action

On September 25, 2024, the Payment Systems Regulator (PSR) announced that it would lower the total coverage for authorized push payment scams.

The regulatory entity states the decision came after careful consideration of feedback and claimed that 99% of APP fraud claims would still be covered. However, the UK Chartered Trading Standards Institute (CTSI) disputed the change, stating that the cap on the Mandatory APP Reimbursement Scheme is too low.

The UK Chartered Trading Standards Institute cited estimates from the National Trading Standards (NTS) Scams Team that fraud costs UK consumers billions annually. Despite other avenues to rectify the matter, victims face additional strain during the process after having already been defrauded. As a result, the CTSI called on the PSR to reinstate the cap to its original level after a promised 12-month review.

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 08, 2024, 05:59 PM

Reference | References

Bleeping Computer
The Hacker News
Bank Info Security
CSO Online
Security Week
Infosecurity Magazine
Security Week

Tags

Qualcomm Flaws, Apache Avro SDK Flaw, Trinity Ransomware, Critical Infrastructure Attacks, Fraud, Data Breaches, Healthcare Sector, malware attack, Ransomware

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

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