Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : 4735bf36 | Oct 07, 2024, 07:49 AM

Today's Headlines:

Leading Story

- Privilege Escalation and Remote Code Execution Threaten Cisco Routers: No Updates Available

Data Breaches & Data Leaks

- Sensitive Data on 61K+ Patients Accessed in Alabama Hospital Cyberattack
- Comcast and Truist Bank Customers Caught Up in FBCS Data Breach

Cyber Crimes & Incidents

- Microsoft and DOJ Seized The Attack Infrastructure Used By Russia-Linked Callisto Group
- Detroit-Area Government Services Impacted By Cyberattack

Vulnerabilities & Exploits

- Apple Releases Critical iOS and iPadOS Updates To Fix VoiceOver Password Vulnerability

Trends & Reports

- Nothing to Report

Privacy, Legal & Regulatory

- Sellafield Fined for Cybersecurity Failures at Nuclear Site

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

Privilege Escalation and Remote Code Execution Threaten Cisco Routers: No Updates Available

Summary

- Cisco warns about two flaws, CVE-2024-20393 and CVE-2024-20470, in routers that will not receive patches as they have passed their end-of-life maintenance.

Analysis & Action

Cisco has identified two vulnerabilities in its Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers, which could expose businesses to security risks.

The vulnerabilities CVE-2024-20393 (CVSS score 8.8) and CVE-2024-20470 (CVSS score 4.7) allow remote attackers to escalate privileges and execute arbitrary commands on the affected devices. The vulnerabilities are rooted in the web-based management interface, which improperly discloses sensitive information. The affected devices have passed their end-of-life maintenance and will not receive patches, and there are no available workarounds to cover these flaws.

Health-ISAC advises those with vulnerable Cisco routers to immediately disable the remote management feature to reduce exposure and to, as a general practice, replace all end-of-life devices with supported alternatives to avoid having vulnerable devices in their environments.

Data Breaches & Data Leaks

Sensitive Data on 61K+ Patients Accessed in Alabama Hospital Cyberattack

Summary

- An Alabama hospital informed more than 61,000 patients that their personal information had been compromised in a cyberattack last year.

Analysis & Action

On October 29, 2023, Medical Center Barbour detected a cyberattack that is assessed to have exposed several patient records.

According to an official letter about the incident, the intruder likely accessed patients' names, dates of birth, home addresses, health insurance information, medical information, and driver's licenses or state IDs. A small subset of individuals' Social Security numbers, passport information, and financial data were also accessed for the impacted patients.

Health-ISAC recommends that organizations implement comprehensive cybersecurity training programs that cover topics such as phishing awareness, secure password practices, data handling procedures, and incident response protocols to mitigate the risk of exposing sensitive data caused by a cyberattack.

Comcast and Truist Bank Customers Caught Up in FBCS Data Breach

Summary

- Comcast Cable Communications and Truist Bank fall victim to a third-party breach at Financial Business and Consumer Solutions (FBCS).

Analysis & Action

Comcast Cable Communications and Truist Bank have been affected by a third-party breach that started with Financial Business and Consumer Solutions (FBCS), a US debt collection agency.

The breach occurred in February when threat actors breached FBCS's network and gained access to electronic records containing names, social security numbers, driver's license numbers, ID cards, dates of birth, and account information of affected individuals. It was thought that the breach initially affected 1.9 million people, but in July, it was concluded that 4.2 million individuals were affected. FBCS's internal investigation is ongoing, and entities indirectly affected must undertake notification and remediation processes themselves, which is what Comcast Cable Communications and Truist Bank are currently doing.

Health-ISAC recommends implementing rigorous vendor risk assessment procedures and having an incident response plan in place to ensure business continuity in cases where third-party partners might be breached.

Cyber Crimes & Incidents

Microsoft And DOJ Seized The Attack Infrastructure Used By Russia-Linked Callisto Group

Summary

- Over 100 domains have been reported to be seized by both the DOJ and Microsoft, used by Russian threat actor Callisto Group

Analysis & Action

Callisto Group, also known by various other names, such as SEABORGIUM and COLDRIVER, focused its attacks on U.S. government and nonprofit organizations and services.

Recent events report, however, that 41 domains have been seized by the Justice Department, along with an additional 66 being restrained in the DOJ's coordinated operations with Microsoft. Further analysis confirmed the threat actor had targeted mainly U.S. entities like the Department of State, Defense, and Energy, along with military defense contractors. The threat group has also committed instances of phishing and data theft for cyberespionage purposes as Callisto's APT group had its targets on NATO countries. More recent statements from Microsoft express their understanding that the group is not completely stopped and will continue establishing new infrastructure.

Health-ISAC recommends consistently monitoring critical infrastructure and unexpected behavior to avoid cyber espionage campaigns. Additionally, including endpoint protections and encryption practices can help act against potential phishing campaigns.

Detroit-Area Government Services Impacted By Cyberattack

Summary

- A recent cyberattack has caused government websites in Wayne County, Michigan, to shut down, and operations of multiple services have been limited.

Analysis & Action

The county is aware of the incident and is following through with investigations, including the FBI and the state police.

Upon launching investigations, the county's information technology team identified that the incident had targeted some of their internal systems due to a recent ransomware attack. The attack began on Wednesday, now creating difficulties for the processing of inmates at the Sheriff's Office. Additionally, the ransomware attacks have limited the ability of real estate leaders to complete work.

Health-ISAC recommends protecting backup files, installing antiviruses, securing endpoints, and limiting users' access privileges. Additionally, regular security testing and network segmentation practices are recommended to limit the chances of future ransomware attacks.

Vulnerabilities & Exploits

Apple Releases Critical iOS and iPadOS Updates To Fix VoiceOver Password Vulnerability

Summary

- Apple fixes two flaws in iOS and iPadOS apps, tracked as CVE-2024-44204 and CVE-2024-44207.

Analysis & Action

One of the flaws tracked as CVE-2024-44204 could allow passwords to be read aloud by VoiceOver assistive technology. Another patched vulnerability, CVE-2024-44207, allows audio to be captured for a couple of seconds before the microphone indicator appears on the screen.

Both issues have been resolved. Apple users are advised to keep automatic updates on to ensure their devices are updated promptly.

Trends & Reports

Nothing to Report.

Privacy, Legal & Regulatory

Sellafield Fined for Cybersecurity Failures at Nuclear Site

Summary

- A British government-owned nuclear facility faces fines for failing to secure information technology systems.

Analysis & Action

The Westminster Magistrates Court issued a fine against Sellafield Ltd following the Office for Nuclear Regulation's (ONR) taking enforcement action in the form of a notice of prosecution on cybersecurity.

The issue was identified after staff at an external site discovered they could access Sellafield's servers and subsequently reported it to the Office for Nuclear Regulation (ONR).

The fines against Sellafield Ltd stem from security failings regarding its information technology systems between 2019 and 2023.

Health-ISAC recommends that organizations implement appropriate security measures to ensure compliance with regulatory requirements and avoid associated fines.

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 07, 2024, 05:59 PM

Reference | References

Cisco
Infosecurity Magazine
Security Affairs
Security Online
The Record
The Hacker News
The Register
Bleeping Computer

Tags

Cybersecurity Failures, Russia-Linked Callisto Group, Cisco Router, Data Breaches, Apple Products

---

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