Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : 0c8b11ab | Oct 01, 2024, 07:38 AM

Today's Headlines:

Leading Story

- Critical WatchGuard Vulnerabilities Discovered: CVE-2024-6592 and CVE-2024-6593

Data Breaches & Data Leaks

- Accounting Firm WMDDH Discloses Data Breach Impacting 127,000
- Hawaii Health Center Discloses Data Breach After Ransomware Attack

Cyber Crimes & Incidents

- French News Agency Faces Major Security Breach
- GorillaBot Emerged As King For DDoS Attacks With 300,000+ Commands

Vulnerabilities & Exploits

- Nothing to Report

Trends & Reports

- Windows 11 KB5043145 Update Causes Reboot Loops, Blue Screens

Privacy, Legal & Regulatory

- US Charges 3 Iranians Over Presidential Campaign Hacking

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

Critical WatchGuard Vulnerabilities Discovered: CVE-2024-6592 and CVE-2024-6593

Summary

- Two critical flaws affecting WatchGuard's Authentication Gateway and Single Sign-On Client software have been identified; immediate patching is advised.

Analysis & Action

A Cybersecurity firm RedTeam Pentesting GmbH, has identified two critical vulnerabilities in WatchGuard's Authentication Gateway and Single Sign-On Client software.

The first vulnerability, CVE-2024-6593, allows an attacker to execute restricted management commands, potentially stealing sensitive user information. The second vulnerability, CVE-2024-6593, involves incorrect authorization in the communication protocol between the Authentication Gateway and Single Sign-On Client, allowing forgery and unauthorized access. Both flaws have a CVSS score of 9.1.

There is currently no reported exploitation, however, due to the widespread use of the WatchGuard software, these flaws could potentially affect thousands of organizations. The company has released fixes, and Health-ISAC recommends users immediately patch their vulnerable devices.

Data Breaches & Data Leaks

Accounting Firm WMDDH Discloses Data Breach Impacting 127,000

Summary

- Over 127,000 individuals' personal information was exposed in a data breach suffered by accounting firm Wright, Moore, DeHart, Dupuis & Hutchinson.

Analysis & Action

The accounting firm recently distributed notification letters to impacted individuals, advising that the incident was identified on July 11, 2023, citing anomalous network activity.

Significant delays in the distribution of the notifications stem from excessive time spent determining who the compromised personal information belonged to and identifying the contact information of those impacted.

According to the investigation, affected personal information included names, Social Security numbers, driver's license numbers, passport numbers, financial account numbers, and medical and treatment information. Health-ISAC recommends implementing a comprehensive security strategy, including strong access controls, employee training, and incident response planning, to safeguard sensitive information from unauthorized access and compromise.

Hawaii Health Center Discloses Data Breach After Ransomware Attack

Summary

- A LockBit data breach at a community clinic in Hawaii has led to 120,000 individuals being impacted in last week's cyberattack.

Analysis & Action

A LockBit cyberattack on Community Clinic of Maui in Hawaii last week breached over 120,000 people's data within a week. The organization's website recently released a data breach notice providing more details on the incident.

Amongst the information that the threat actor has compromised were social security numbers, date of birth, driver's license numbers, bank and payment information, names, login information, and sensitive medical information. Currently, the clinic is unsure how the exposed information will be misused. The clinic has offered credit monitoring services to impacted personnel in light of the attacks. Uncertainty remains on what LockBit will do with the breached information, but the likelihood remains that they will use it for monetary gain.

Threat actors continue to utilize forms of data breaches and leaks for monetary gain, shining light

on the need for preventative measures. Health-ISAC recommends using trusted anti-malware software and data encryption methods to prevent further instances of data breaches going forward.

Cyber Crimes & Incidents

French News Agency Faces Major Security Breach

Summary

- An unknown threat actor has targeted the French news agency Agence France-Presse (AFP), causing disruptions to some systems and transmissions.

Analysis & Action

The French news agency Agence France-Presse (AFP) suffered a cyberattack that disrupted its information systems and client transmission technologies. The agency has assured that its global news coverage will continue uninterrupted.

The perpetrators' identity and motives remain unknown. The cyberattack is part of a broader trend of rising cybersecurity threats targeting critical infrastructure and media outlets globally. Last year, the agency was a victim of an attack by the hacktivist group Anonymous Sudan. Earlier this year, Poland's state news agency attack was suspected to be linked to Russian intelligence, demonstrating that threat actors with various motivations, including political or geopolitical motives, can target media outlets.

The agency's technical teams are working with the National Authority for Information Security (ANSSI) to handle the breach and return operations to normal. The increase in cyberattacks on media outlets underscores the necessity for improved security defenses and increased collaboration with relevant national cybersecurity entities and law enforcement.

GorillaBot Emerged As King For DDoS Attacks With 300,000+ Commands

Summary

- In recent discoveries, analysts uncovered the leading botnet, GorillaBot, possessing over 300,000 commands.

Analysis & Action

The GorillaBot botnet was discovered to be a modified version of the Mirai malware campaign. The botnet utilizes compromised devices to send various requests to targets to block resources and bandwidth.

In just twenty-four days, the botnet distributed over 300,000 DDoS attacks, targeting 113 countries. Amongst the highest impacted were China (20%), The United States (19%), and Canada (16%). GorillaBot targets sectors like telecommunications, banks, universities, and government websites, to name a few. Additionally, the botnet can utilize a vast amount of CPU architecture like x86, MIPS, ARM, and x86_64. UDP Flood remains the most common of the botnet attack methods at 41%, followed by ACK BYPASS FLOOD at 24%. Several IOCs have been identified regarding the botnet to help crack down on its malicious intentions.

As threat actors continue to heavily utilize botnets, awareness must be raised about the risks they present. Health-ISAC recommends using trusted antivirus software and installing consistent updates for operating systems and software.

Vulnerabilities & Exploits

- Nothing to Report

Trends & Reports

Windows 11 KB5043145 Update Causes Reboot Loops, Blue Screens

Summary

- Microsoft has issued a warning about a recent Windows 11 update that could cause systems to freeze or restart repeatedly.

Analysis & Action

The optional KB5043145 update, released this month, was intended to fix various issues but has instead led to problems for some users.

After installing the update, affected users reported that their computers were entering restart loops or becoming unresponsive with blue or green screens. Some devices have even automatically opened the Automatic Repair tool or triggered BitLocker recovery.

Microsoft is currently investigating the issue. Health-ISAC-affected members are recommended to report it through the Feedback Hub. The company has also acknowledged similar boot issues in previous updates, including those released in August and June.

Privacy, Legal & Regulatory

US Charges 3 Iranians Over Presidential Campaign Hacking

Summary

- Charges have been brought against three Islamic Revolutionary Guard Corps (IRGC) employees for their involvement in a cyber campaign targeting US presidential elections.

Analysis & Action

Recently, the US Justice Department levied charges against three employees of Iran's Islamic Revolutionary Guard Corps (IRGC) for their involvement in cyber attacks against presidential campaigns, former US officials, non-governmental organizations (NGOs), and members of the media.

The three IRGC employees, identified as Masoud Jalili, Seyyed Ali Aghamiri, and Yaser Balaghi, have been charged with conspiracy to commit identity theft, aggravated identity theft, unauthorized access to computers, access device fraud, and wire fraud.

According to the Department of Justice, the individuals have been involved in IRGC hacking campaigns since at least January 2020, executing spear-phishing, social engineering, and other techniques in an attempt to compromise computers and accounts. Health-ISAC recommends that organizations remain vigilant as the elections provide adversaries with an opportunity to leverage operations to sway public interests via disinformation and misinformation campaigns or cyber-attacks that cause disruptions to critical infrastructure with a nexus to healthcare.

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 01, 2024, 11:59 PM

Reference | References

thecyberexpress
Security Week
Bleeping Computer
Microsoft Blog
cybersecuritynews
Security Online
Security Week
Security Week

Tags

Windows 11 KB5043145, GorillaBot, WMDDH, CVE-2024-6593, CVE-2024-6592, IRGC

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