Health-ISAC™

Collaborating for Resilience in Healthcare

Daily Cyber Headlines

Daily Cyber Headlines ○ TLP:WHITE Alert ID : 860f2ccb Oct 09, 2024, 08:00 AM

Today's Headlines:

Leading Story

- Microsoft Issues Security Update Fixing 118 Flaws, Two Actively Exploited in the Wild

Data Breaches & Data Leaks

- Nothing to Report

Cyber Crimes & Incidents

- ESET Research: GoldenJackal APT Group, With Air-Gap-Capable Tools, Targets Systems In Europe To Steal Confidential Data
- AT&T, Verizon Reportedly Hacked to Target US Govt Wiretapping Platform

Vulnerabilities & Exploits

- PoC Exploit Releases For CVE-2023-52447: A Linux Kernel Flaw Enabling Container Escape
- Ivanti Warns of Three More CSA Zero-Days Exploited in Attacks

Trends & Reports

- Cloud Security Risks Surge as 38% of Firms Face Exposures
- Microsoft Detects Growing Use of File Hosting Services in Business Email Compromise Attacks

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 – 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

Microsoft Issues Security Update Fixing 118 Flaws, Two Actively Exploited in the Wild

Summary

- Microsoft patches two exploited flaws in October Patch Tuesday.

Analysis & Action

Microsoft released security updates during October Patch Tuesday to fix 118 vulnerabilities, two actively exploited in the wild.

The vulnerabilities range from critical to moderate severity. Two exploited flaws are Microsoft Management Console Remote Code Execution Vulnerability CVE-2024-43572, with a CVSS score of 7.8, and Windows MSHTML Platform Spoofing Vulnerability CVE-2024-43573, with a CVSS score of 6.5. It is currently unknown how or by whom these vulnerabilities are exploited.

Health-ISAC recommends immediate patching of Microsoft devices to minimize the risk of exploitation.

Data Breaches & Data Leaks

Nothing to Report.

Cyber Crimes & Incidents

ESET Research: GoldenJackal APT Group, With Air-Gap-Capable Tools, Targets Systems In Europe To Steal Confidential Data

Summary

- Attacks spanning from May 2022 to March 2024 have been discovered in Europe, APT group utilized tools targeting air-gapped systems

Analysis & Action

Recent discoveries have revealed that the advanced persistent threat (APT) group GoldenJackal is behind several attacks in Europe. The APT group mainly targets diplomatic and governmental entities.

ESET research shows that one of the group's attacks involved using their custom toolset. With this custom toolset, the group could target systems air-gapped at the South Asian embassy. Another attack from the group involved a modular toolset, where a government organization in the European Union country was targeted. Research points to the group seeking confidential information for processing, distribution, exfiltrating, and commanding to separate systems, mainly targeting high-profile machines explaining their focus on air-gapped systems. As the difficulty level of deploying more than one toolset to compromise air-gapped systems is high, the actor is a high-intelligence threat.

Threat actors continue to develop more sophisticated attack methods, highlighting the importance of security measures to protect confidential information. Health-ISAC recommends using secure offline strategies, platforms, and air gap backups to diminish the chances of similar attacks.

AT&T, Verizon Reportedly Hacked To Target US Govt Wiretapping Platform

Summary

- Chinese-linked Salt Typhoon breached U.S. Internet providers for a suspected cyber espionage operation.

Analysis & Action

Salt Typhoon, a Chinese hacking group, has breached multiple U.S. broadband providers, including Verizon, AT&T, and Lumen Technologies. The group has been active since at least 2019 and has targeted victims globally, with a special focus on Southeast Asian entities.

It is presumed that the threat actors conducted the attack for cyberespionage purposes, as they had access to systems used by the U.S. federal government for court-authorized network wiretapping requests. The investigation of the incident is still ongoing, and it is currently unknown what data, if any, was breached or exfiltrated. While not confirmed, some experts suspect Cisco devices used to route internet traffic might have been used for initial access.

Health-ISAC advises members to patch vulnerable devices consistently and stay updated on the evolving threat landscape by understanding active threat actors and their TTPs.

Vulnerabilities & Exploits

PoC Exploit Release For CVE-2023-52447: A Linux Kernel Flaw Enabling Container Escape

Summary

- A proof of concept exploit has been published regarding a vulnerability in the Linux Kernel, tracked as CVE-2023-52447

Analysis & Action

CVE-2023-52447 has been discovered to be a use-after-free flaw. It is located in the BPF subsystem of Linux's Kernel and pertains to the process of using array map pointers and their management in programs with BPFs.

The vulnerability has received a CVSS score of 7.8, affecting versions v5.8 to v6.6, posing serious concerns for any system that may depend on the method of containerization for their isolation of security. This issue occurs when the BPF program holds the pointer for an array map from array_of_maps while the reference counts are not increased properly. The time consumption of the operation gives time for another thread to free, allowing for the use-after-free flaw to take place. The proof-of-concept has since been posted to GitHub so that security teams can research and understand the vulnerability and its exploits. Recent kernel patches have since addressed the vulnerability as organizations are asked to update to the latest kernel patch to ensure their safety.

Health-ISAC recommends updating systems using the most recent patches to ensure minimal exposure to the vulnerabilities addressed in this instance.

Ivanti Warns of Three More CSA Zero-Days Exploited in Attacks

Summary

- Ivanti has issued security updates to address three newly discovered zero-day vulnerabilities in its Cloud Services Appliance (CSA) product.

Action & Analysis

Attackers actively exploit these vulnerabilities (CVE-2024-9379, CVE-2024-9380, or CVE-2024-9381) to gain unauthorized access to sensitive systems. As Ivanti disclosed, the attackers combined these three vulnerabilities with a previously patched CSA zero-day to execute a series of malicious actions. Successful exploitation of these vulnerabilities could allow attackers to inject malicious SQL code, execute arbitrary commands, and bypass security restrictions.

Ivanti has warned that customers running CSA 4.6 patch 518 or earlier are particularly at risk if they have not applied the necessary security updates. The company recommends that affected customers immediately upgrade to CSA 5.0.2 to mitigate the risk of exploitation.

Health-ISAC recommends administrators closely monitor their systems for unusual activity, such as new or modified admin accounts or alerts from endpoint detection and response (EDR) software.

Trends & Reports

Cloud Security Risks Surge as 38% of Firms Face Exposures

Summary

- A new report warns of increasing cloud security risks, with 38% of organizations globally facing critical vulnerabilities.

Analysis & Action

According to a report by Tenable, the risks many organizations face regarding cloud infrastructure are due to publicly exposed, critically vulnerable, and highly privileged cloud workloads. This combination makes them susceptible to cyberattacks that could lead to application disruptions, system takeovers, and costly data breaches.

The report highlights telemetry data captured during the first half of 2024, including misconfigurations, risky entitlements, and persistent vulnerabilities in areas such as identities and permissions, storage, workloads, and containers.

The findings underscore the urgent need for organizations to address these risks to prevent devastating breaches. One key takeaway is that the issues may not always stem from threat actor operations and that, in many cases, misconfigurations or over-privileged access represent the highest risk for cloud data exposures. Health-ISAC recommends that organizations regularly assess their security apparatus to discover any potential security gaps to mitigate their existence within their network and reduce the risk of threat actors taking advantage of the flaw.

Microsoft Detects Growing Use of File Hosting Services in Business Email Compromise Attacks

Summary

- Microsoft has identified a malicious campaign using legitimate file hosting services to blend in and evade detection.

Analysis & Action

Microsoft is warning of cyber attack campaigns exploiting legitimate file hosting services like SharePoint, OneDrive, and Dropbox. This technique, also called living-off-trusted-sites (LOTS), is a tactic that allows attackers to blend in with internet traffic and ultimately aids them in evading detection.

These campaigns allow threat actors to compromise devices and credentials, conduct business email compromise (BEC) attacks, and potentially result in financial fraud, data exfiltration, and lateral movement. The weaponization of legitimate internet services (LIS) is an increasingly popular threat across industries, adopted by adversaries to circumvent traditional security defense tools and complicate attribution efforts.

Health-ISAC recommends reading CISA’s guide, Identifying and Mitigating Living Off the Land Techniques, to learn how to prevent an attack with threat actors using legitimate services to conceal a breach.

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 09, 2024, 05:59 PM

Reference | References

Bleeping Computer

The Hacker News
CISA
ESET
Infosecurity Magazine
Security Online
The Hacker News
Bleeping Computer

Tags

Linux Kernel Flaw, GoldenJackal APT Group, Salt Typhoon, Ivanti CSA Flaw, living-off-the-land tactics, Microsoft Patch Tuesday, Cloud Security

---

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