HC3: Monthly Cybersecurity Vulnerability Bulletin
October 05, 2023 TLP:CLEAR Report: 202310051200

September Vulnerabilities of Interest to the Health Sector

In September 2023, vulnerabilities to the health sector have been released that require attention. This includes the monthly Patch Tuesday vulnerabilities released by several vendors on the second Tuesday of each month, along with mitigation steps and patches. Vulnerabilities for September are from Microsoft, Google/Android, Cisco, Apple, Mozilla, SAP, Fortinet, VMWare, Progress Software, and Adobe. A vulnerability is given the classification as a zero-day when it is actively exploited with no fix available or if it is publicly disclosed. HC3 recommends patching all vulnerabilities with special consideration to the risk management posture of the organization.

Importance to the HPH Sector

Department Of Homeland Security/Cybersecurity & Infrastructure Security Agency

The Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) added a total of 23 vulnerabilities in September to their Known Exploited Vulnerabilities Catalog.

This effort is driven by Binding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities, which established the Known Exploited Vulnerabilities Catalog as a living list of known CVEs that carry significant risk to the U.S. federal enterprise.

Vulnerabilities that are entered into this catalog are required to be patched by their associated deadline by all U.S. executive agencies. While these requirements do not extend to the private sector, HC3 recommends all healthcare entities review the vulnerabilities in this catalog and consider prioritizing them as part of their risk mitigation plan. The full database can be found here.

Microsoft

Microsoft released or provided security updates for 96 vulnerabilities, including two actively exploited zero-days. Seven of these vulnerabilities were listed as critical; six were remote code execution flaws, with the highest one tracked as CVE-2023-38148, which is an Internet Connection Sharing (ICS) RCE vulnerability. The remaining critical vulnerability allows an elevation of privilege in the Azure Kubernetes Service. The two zero-day vulnerabilities were either exploited in attacks or publicly disclosed. Additional information on these exploits can be found below:

- CVE-2023-36802: (Microsoft Streaming Service Proxy Elevation of Privilege Vulnerability) - Microsoft has fixed this actively exploited local privilege elevation vulnerability which allows threat actors to gain SYSTEM privileges.
- CVE-2023-36761: (Microsoft Word Information Disclosure Vulnerability) - Microsoft has fixed an actively exploited vulnerability that can be used to steal NTLM hashes when opening a document, including in the preview panel. These NTLM hashes can be cracked or used in NTLM Relay attacks to gain access to the account.

For a complete list of Microsoft vulnerabilities and security updates, click here. HC3 recommends all users follow Microsoft's guidance, which is to refer to Microsoft's Security Response Center and apply the

necessary updates and patches immediately, as these vulnerabilities can adversely impact the health sector.

Google/Android

Google/Android released two updates early in September which addressed 33 vulnerabilities, including a zero-day that was potentially exploited in the wild. This high-severity zero-day, tracked as CVE-2023-35674, is a bug inside of the Android Framework that allows threat actors the ability to escalate privileges without requiring user interaction or additional execution privileges. According to a Google advisory: "There are indications that CVE-2023-35674 may be under limited, targeted exploitation."

Of the 33 flaws fixed, three of these were rated as critical, CVE-2023-35658, CVE-2023-35673, and CVE-2023-35681, and can all lead to remote code execution with no additional user interaction required for exploitation. Ten of the vulnerabilities were given a high security rating and can result in an unauthorized escalation of privileges. This update also addresses a vulnerability which can lead to a denial of service through either a factory reset or continuously locking the device (CVE-2023-35677). In their second update, released on September 5, 2023, Google/Android addressed vulnerabilities in Qualcomm components. The most critical of these is tracked as CVE-2023-28581, which is a WLAN firmware memory corruption that can allow attackers to execute arbitrary code. Towards the end of September, Google also updated their Chrome browser to fix 10 vulnerabilities, including one high-impact exploit tracked as CVE-2023-5217, which can allow for a heap buffer overflow in the vp8 encoding in libvpx, a software video codec from Google and the Alliance for Open Media.

HC3 recommends users refer to the Android and Google service mitigations section for a summary of the mitigations provided by Android security platform and Google Play Protect, which improves the security of the Android platform. It is imperative that health sector employees keep their devices updated and apply patches immediately, and those who use older devices follow previous guidance to prevent their devices from being compromised. All Android and Google service mitigations along with security information on vulnerabilities for the month of September can be viewed by clicking here, and the Chrome browser update can be viewed here.

Apple

Apple released security updates to address vulnerabilities in multiple products, along with three new zero-day vulnerabilities which have been previously exploited. According to researchers, attackers were able to exploit an iPhone zero-day chain (CVE-2023-41991, CVE-2023-41992, and CVE-2023-41993). CVE-2023-41993 was used for initial remote code execution in Safari by creating malicious web pages. Following with CVE-2023-41991 to bypass signature validation, CVE-2023-41992 was used for privilege escalation to access the kernel. To mitigate this risk, Apple has released updates for multiple products to patch this vulnerability. Apple has also addressed vulnerabilities in other products, which could allow an attacker to take control of an affected device. HC3 recommends all users and administrators follow CISA's guidance, which encourages users and administrators to review the following advisories and apply the necessary updates:

- iOS 15.7.9 and iPadOS 15.7.9
- macOS Monterey 12.6.9
- macOS Big Sur 11.7.10

- iOS 17.0.1 and iPadOS 17.0.1
- iOS 16.7 and iPadOS 16.7
- watchOS 10.0.1
- watchOS 9.6.3
- Safari 16.6.1
- macOS Ventura 13.6
- macOS Monterey 12.7

For a complete list of the latest Apple security and software updates, click here. HC3 recommends all users install updates and apply patches immediately. It is worth noting that after a software update is installed for iOS, iPadOS, tvOS, and watchOS, it cannot be downgraded to the previous version.

Mozilla

Mozilla released security advisories in September addressing vulnerabilities affecting multiple Mozilla products, including Firefox, Firefox ESR, Thunderbird, Firefox Focus for Android, and Firefox for Android. If successful, a threat actor could exploit these vulnerabilities to take control of a compromised system or device. HC3 encourages all users to follows CISA's guidance to review the following advisories and apply the necessary updates:

- Thunderbird 115.3
- Firefox ESR 115.3
- Firefox 118
- Mozilla Foundation Security Advisory 2023-40 (Security Vulnerability fixed in Firefox 117.0.1, Firefox ESR 115.2.1, Firefox ESR 102.15.1, Thunderbird 102.15.1, and Thunderbird 115.2.2)
- Mozilla Foundation Security Advisory 2023-44 (Security Vulnerability fixed in Firefox 118.0.1, Firefox ESR 115.3.1, Firefox for Android 118.1.0, Firefox Focus for Android 118.1.0, and Thunderbird 115.3.1)

A complete list of Mozilla's updates including lower severity vulnerabilities are available on the Mozilla Foundation Security Advisories page. HC3 recommends applying the necessary updates and patches immediately, and follow Mozilla's guidance for additional support.

Cisco

Cisco released security updates to address vulnerabilities in multiple products. Two were classified as "Critical" in severity, eight as "High," and 15 as "Medium" in severity. If successful, a cyber threat actor can exploit some of these vulnerabilities to take control of an affected device or system. HC3 encourages users follow CISA's guidance and review the following advisories:

- BroadWorks and BroadWorks Xtended
- Identity Services Engine RADIUS
- Android Framework Privilege Escalation Vulnerability (CVE-2023-35674)
- Cisco Adaptive Security Appliance and Firepower Threat Defense Unauthorized Access Vulnerability (CVE-2023-20269)
- Google Chrome Heap-Based Buffer Overflow Vulnerability (CVE-2023-4863)

- Cisco Catalyst SD-WAN Manager Vulnerabilities
- Cisco IOS XE Software Web UI Command Injection Vulnerability
- Cisco IOS XE Software for ASR 1000 Series Aggregation Services Routers IPv6 Multicast Denial of Service Vulnerability
- Cisco IOS XE Software Layer 2 Tunneling Protocol Denial of Service Vulnerability
- Cisco DNA Center API Insufficient Access Control Vulnerability
- Cisco IOS XE Software for Catalyst 3650 and Catalyst 3850 Series Switches Denial of Service Vulnerability
- Cisco IOS XE Software Application Quality of Experience and Unified Threat Defense Denial of Service Vulnerability
- Cisco IOS and IOS XE Software Command Authorization Bypass Vulnerability

HC3 recommends applying the necessary patches and updates immediately. For a complete list of Cisco security advisories released in September, visit the Cisco Security Advisories page by clicking here. Cisco also provides free software updates that address critical and high-severity vulnerabilities listed in their security advisory.

SAP

SAP released 13 new security notes and five updates to previously issued security notes, to address vulnerabilities affecting multiple products. If successful in launching an attack, a threat actor could exploit these vulnerabilities and take control of a compromised device or system. This month there were five vulnerabilities with a severity rating of "Hot News" which is the most severe and a top priority for SAP. There were also two flaws rated as "High", nine "Medium," and two "Low" in severity. A breakdown of some security notes for vulnerabilities with a "Hot News" severity rating are as follows:

- **Security Note #2622660:** (No CVE Associated) This is an update to a security note released back on April 2018, which includes security updates for the browser control Google Chromium delivered with SAP Business Client. Product impacted: SAP Business Client, Versions - 6.5, 7.0, 7.70.
- **Security Note #3320355:** (CVE-2023-49622) This an Information Disclosure vulnerability in SAP BusinessObjects Business Intelligence Platform (Promotion Management). Product impacted: SAP BusinessObjects Business Intelligence Platform (Promotion Management), Versions– 420,430.
- **Security Note #3273480:** (CVE-2022-41272) This an update to a security note released during December 2022's Patch Day. This is an Improper access control in SAP NetWeaver AS Java (User Defined Search). Product impacted: SAP NetWeaver Process Integration, Version –7.50.

For a complete list of SAP's security notes and updates for vulnerabilities released in September, click here. HC3 recommends following the manufacturer's guidance by visiting the Support Portal and applying any necessary patches to protect their SAP landscape.

VMWare

In September, VMWare released two security updates addressing vulnerabilities in VMware Tools and Aria

Operations. A remote attacker could exploit some of these vulnerabilities to take control of an affected system. Additional information on each is as follows:

- VMSA-2023-0019.1 (CVE-2023-20900): Has a CVSSv3 base score of 7.5 and is rated as important in severity. This is a SAML token signature bypass vulnerability in VMware Tool. If successful, a threat actor that has been granted Guest Operation Privileges in a target virtual machine may be able to elevate their privileges if that target virtual machine has been assigned a more privileged Guest Alias. To remediate CVE-2023-20900, apply the patches listed in the 'Fixed Version' column of the 'Response Matrix', which can be accessed by clicking here.
- VMSA-2023-0023 (CVE-2023-34043): Has a CVSSv3 base score of 6.7 and is moderate in severity. This is a local privilege escalation vulnerability affecting Aria Operations. If successful, a remote threat actor with administrative access to the local system can escalate privileges to 'root'. To remediate CVE-2023-34043, apply the updates listed in the 'Fixed Version' column of the 'Response Matrix', which can be accessed by clicking here.

For a complete list of VMWare's security advisories, click here. Patches are available to remediate these vulnerabilities found in VMWare products. HC3 recommends users follow VMWare's guidance for each and applying patches listed in the 'Fixed Version' column of the 'Response Matrix' that can be accessed by clicking directly on the security advisory.

Adobe

Adobe released security advisories to address multiple vulnerabilities in Adobe software. If successful, a threat actor could exploit some of these vulnerabilities to take control of an affected system. HC3 recommends that all users review the Adobe Security Bulletins and apply any necessary updates:

- Adobe Connect: APSB23-33
- Adobe Acrobat and Reader: APSB23-34
- Adobe Experience Manager: APSB23-43

For a complete list of Adobe security updates, click here. HC3 recommends all users apply necessary updates and patches immediately.

Fortinet

Fortinet's September vulnerability advisory addressed several vulnerabilities across different Fortinet products, including vulnerabilities (CVE-2023-29183 and CVE-2023-34984) affecting FortiOS, FortiProxy, and FortiWeb. If successful, a threat actor can exploit this vulnerability and take control of a compromised device or system. HC3 recommends all users review Fortinet's security advisories FG-IR-23-106 and FG-IR-23-068, along with Fortinet's September 2023 Vulnerability Advisories page for additional information, and apply all necessary updates and patches immediately.

Progress Software

Progress Software released an advisory regarding multiple vulnerabilities in their WS_FTP Server. Two of these vulnerabilities were rated as critical and are being tracked as CVE-2023-40044 and CVE-2023-4265. CVE-2023-40044 affects versions prior to 8.7.4 and 8.8.2, allowing a pre-authenticated attacker to leverage a .NET deserialization vulnerability in the Ad Hoc Transfer module to execute remote commands on the

underlying WS_FTP Server operating system. CVE-2023-4265 is a directory traversal vulnerability that impacts the same versions. If successfully exploited, an attacker could leverage this to perform file operations (delete, rename, rmdir, mkdir) on files and folders that are outside of the authorized WS_FTP path. Additionally, the attacker could escape the WS_FTP server file structure and perform the same operations on the operating system. Additional security information from Progress Software and their products can be viewed here.

References

Adobe Releases Security Updates for Multiple Products
https://www.cisa.gov/news-events/alerts/2023/09/12/adobe-releases-security-updates-multiple-products

Android Security Bulletins
https://source.android.com/security/bulletin

Apple Releases Security Updates for Multiple Products
https://www.cisa.gov/news-events/alerts/2023/09/22/apple-releases-security-updates-multiple-products

Apple Releases Security Updates for iOS and macOS
https://www.cisa.gov/news-events/alerts/2023/09/12/apple-releases-security-updates-ios-and-macos

Apple Security Releases
https://support.apple.com/en-us/HT201222

Cisco Security Advisories
https://tools.cisco.com/security/center/publicationListing.x

Cisco Releases Security Advisories for Multiple Products
https://www.cisa.gov/news-events/alerts/2023/09/28/cisco-releases-security-advisories-multiple-products

Citizen Lab: Predator in the Wires
PREDATOR IN THE WIRES: Ahmed Eltantawy Targeted with Predator Spyware After Announcing Presidential Ambitions - The Citizen Lab

Fortinet Patches High-Severity Vulnerabilities in FortiOS, FortiProxy, FortiWeb Products
https://www.securityweek.com/fortinet-patches-high-severity-vulnerabilities-in-fortios-fortiproxy-fortiweb-products/

Fortinet Releases Security Updates for Multiple Products
https://www.cisa.gov/news-events/alerts/2023/09/15/fortinet-releases-security-updates-multiple-products

FortiGuard Labs PSIRT Advisories
https://www.fortiguard.com/psirt

Microsoft September 2023 Patch Tuesday fixes 2 zero-days, 59 flaws
https://www.bleepingcomputer.com/news/microsoft/microsoft-september-2023-patch-tuesday-fixes-2-zero-days-59-flaws/

Microsoft September 2023 Patch Tuesday
https://isc.sans.edu/diary/Microsoft+September+2023+Patch+Tuesday/30214/

Microsoft Month Archives: September 2023
https://msrc.microsoft.com/blog/2023/09/

Mozilla Foundation Security Advisory 2023-40
https://www.mozilla.org/en-US/security/advisories/mfsa2023-40/

Mozilla Foundation Security Advisory 2023-44
https://www.mozilla.org/en-US/security/advisories/mfsa2023-44/

Mozilla Releases Security Updates for Multiple Products
https://www.cisa.gov/news-events/alerts/2023/09/29/mozilla-releases-security-updates-multiple-products

Mozilla Releases Security Advisories for Thunderbird and Firefox
https://www.cisa.gov/news-events/alerts/2023/09/27/mozilla-releases-security-advisories-thunderbird-and-firefox

Microsoft Patch Tuesday by Morphus Labs
https://patchtuesdaydashboard.com/

Microsoft Security Update Guide
https://msrc.microsoft.com/update-guide

Mozilla Foundation Security Advisories
https://www.mozilla.org/en-US/security/advisories/

Progress Community
WS_FTP Server Critical Vulnerability - (September 2023) - Progress Community

Progress Security Center
Security Center - Progress

SAP Security Patch Day – September 2023
https://dam.sap.com/mac/app/e/pdf/preview/embed/ucQrx6G?ltr=a&rc=10

SAP Security Notes

https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html

THE SEPTEMBER 2023 SECURITY UPDATE REVIEW
https://www.zerodayinitiative.com/blog/2023/9/12/the-september-2023-security-update-review

September Android updates fix zero-day exploited in attacks
https://www.bleepingcomputer.com/news/security/september-android-updates-fix-zero-day-exploited-in-attacks/

VMware Security Advisories
https://www.vmware.com/security/advisories.html

VMware Releases Security Update for Tools
https://www.cisa.gov/news-events/alerts/2023/09/01/vmware-releases-security-update-tools

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback