Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

HC3: Monthly Cybersecurity Vulnerability Bulletin
August 23, 2023 TLP:CLEAR Report: 202308231200

July Vulnerabilities of Interest to the Health Sector

In July 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 July are from Microsoft, Google/Android, Apple, Mozilla, SAP, Cisco, Fortinet, VMWare, MOVEit, Oracle, and Adobe. A vulnerability is given the classification as a zero-day if 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 16 vulnerabilities in July 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 vulnerabilities in this catalog and consider prioritizing them as part of their risk mitigation plan. The full database can be found here.

Microsoft

Microsoft issued security updates to fix 132 vulnerabilities, including six actively exploited and 37 remote code execution (RCE) flaws for July's Patch Tuesday. According to researchers, this is the largest number of vulnerabilities addressed by the vendor since April 2022. Of the 37 remote code execution vulnerabilities that were fixed, Microsoft only categorized nine vulnerabilities as 'Critical.' According to researchers, one of the RCE flaws remains unpatched and is actively exploited in attacks seen by numerous cybersecurity firms. The number of bugs in each vulnerability category is listed as follows:

- 33 Elevation of Privilege Vulnerabilities
- 13 Security Feature Bypass Vulnerabilities
- 37 Remote Code Execution Vulnerabilities
- 19 Information Disclosure Vulnerabilities
- 22 Denial of Service Vulnerabilities
- 7 Spoofing Vulnerabilities

At this time, Microsoft has not fixed any Microsoft Edge vulnerabilities for the month of July. Additionally, July's Patch Tuesday addressed six zero-day vulnerabilities, all of them exploited in attacks, and one of them publicly disclosed. The six actively exploited zero-day are as follows:

- CVE-2023-32046 - **Windows MSHTML Platform Elevation of Privilege Vulnerability.** Microsoft has fixed an actively exploited privilege elevation vulnerability in Windows MSHTML that was exploited by opening a specially crafted file through email or malicious websites. According to Microsoft, the threat actor “would gain the rights of the user that is running the affected application.”
- CVE-2023-32049 - **Windows SmartScreen Security Feature Bypass Vulnerability.** Threat actors exploited this flaw to prevent the display of the Open File - Security Warning prompt when downloading and opening files from the Internet.
- CVE-2023-36874 - **Windows Error Reporting Service Elevation of Privilege Vulnerability.** This actively exploited elevation of privileges bug allows threat actors to gain administrator privileges on a compromised Windows device. According to Microsoft, “An attacker must have local access to the targeted machine and the user must be able to create folders and performance traces on the machine, with restricted privileges that normal users have by default.”
- CVE-2023-36884 - **Office and Windows HTML Remote Code Execution Vulnerability.** Microsoft released guidance on the publicly disclosed, unpatched Microsoft Office and Windows zero-day that allows remote code execution using specially crafted Microsoft Office documents. With this vulnerability, the threat actor would have to convince the victim to open the malicious file for the attack to launch. According to Microsoft’s advisory, they are aware of and are “investigating reports of a series of remote code execution vulnerabilities impacting Windows and Office products.” After Microsoft’s investigation is complete, the vendor said they will take the necessary steps to protect consumers and “might include providing a security update through our monthly release process or providing an out-of-cycle security update, depending on customer needs." According to Microsoft, the vulnerability is exploited by the RomCom hacking group, previously known to deploy the Industrial Spy ransomware in attacks. The threat actor group continues to extort victims, has rebranded themselves by using the name “Underground,” and are also linked to the Cuba ransomware operation.

For a complete list of Microsoft vulnerabilities released in July and their rating, click here, and for all 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’s July security updates for Android fixed 43 vulnerabilities, including three that have been exploited in attacks. According to Google’s bulletin, “There are indications that the following [vulnerabilities] may be under limited, targeted exploitation.” These three exploited flaws, tracked as CVE-2023-2136, CVE-2023-26083, and CVE-2021-29256, affect Android’s System and Arm Mali components. Additional information of vulnerabilities of note are as follows:

- CVE-2023-2136 is a critical-severity vulnerability with a 9.6 CVSS score that was fixed in April. The flaw is an integer overflow bug in Skia, Google’s open-source multi-platform 2D graphics library that is also used in Chrome. According to Google’s July 2023 Android security bulletin, this vulnerability can be exploited to achieve remote code execution on Android devices.
- CVE-2023-26083 is a medium-severity memory leak flaw in the Arm Mali GPU driver for Bifrost, Avalon, and Valhall chips. This vulnerability was leveraged in an exploit chain that delivered spyware to Samsung devices back in December 2022.

- CVE-2021-29256 is a high-severity vulnerability with a CVSS score of 8.8, that is an unprivileged information disclosure and root privilege escalation flaw impacting specific versions of the Bifrost and Midgard Arm Mali GPU kernel drivers.
- CVE-2023-21250 is the most severe of the security problems that Google fixed this month. This flaw is a critical vulnerability in Android's System component that impacts Android versions 11, 12, and 13. If a threat actor exploits this bug, it could lead to remote code execution with no user interaction or additional execution privilege.

Every month, security updates are released in two parts, or patch levels. The first part, 2023-07-01, addressed core Android components (frameworks), and the second part, 2023-07-05, addressed kernel and closed source components. July's Android security update covers Android versions 11, 12, and 13. However, depending on the vulnerabilities addressed, older OS versions that are no longer supported may be impacted. HC3 recommends users refer to the Android and Google service mitigations section for a summary of the mitigations provided by the Android Security Platform and Google Play Protect, which improve 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 affecting Android devices, can be viewed by clicking here.

Apple

Apple released security updates to address vulnerabilities in multiple products. If successful, a threat actor can exploit some of these vulnerabilities and take control of a compromised device or system. HC3 recommends all users to follow CISA's guidance, which encourages users and administrators to review the following advisories and apply the necessary updates:

- iOS 16.6 and iPadOS 16.6
- iOS 15.7.8 and iPadOS 15.7.8
- macOS Ventura 13.5
- macOS Monterey 12.6.8
- macOS Big Sur 11.7.9
- Safari 16.6
- tvOS 16.6
- watchOS 9.6

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

- Firefox 115 Mozilla Foundation Security Advisory 2023-24
- Firefox ESR 102.13 Mozilla Foundation Security Advisory 2023-23
- Thunderbird 102.13 Mozilla Foundation Security Advisory 2023-22
- Firefox 115.0.2 and Firefox ESR 115.0.2 Mozilla Foundation Security Advisory 2023-26

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 following Mozilla's guidance for additional support.

SAP

SAP released 16 new security notes, and two updates for previously released security notes, to address vulnerabilities affecting multiple products. If successful, a threat actor could exploit these vulnerabilities and take control of a compromised device or system. This month, there were two vulnerabilities rated as "Hot News," seven "High," and nine "Medium" in severity. A breakdown of security notes for vulnerabilities with a "Hot News" severity rating are as follows:

- **Security Note #2622660** has a CVSS score of 10.0 and a "Hot News" severity rating. This is an update to a security note released on April 2018 Patch Day. Security updates for the browser control Google Chromium delivered with SAP Business. Product(s) impacted: AP Business Client, Versions -6.5, 7.0, 7.70.
- **Security Note #3350297** (CVE-2023-36922) has a CVSS score of 9.1 and a "Hot News" severity rating. This is an OS command injection vulnerability in SAP ECC and SAP S/4HANA (IS-OIL). Product(s) impacted: SAP ECC and SAP S/4HANA (IS-OIL), Versions -600, 602, 603, 604, 605, 606, 617, 618, 800, 802, 803, 804, 805, 806, 807.

For a complete list of SAP's security notes and updates for vulnerabilities released in July, click here. HC3 recommends patching immediately and following SAP's guidance for additional support. To fix vulnerabilities discovered in SAP products, SAP recommends customers visit the Support Portal and apply patches to protect their SAP landscape.

Cisco

Cisco released ten security advisories for vulnerabilities affecting multiple Cisco products. One advisory was rated "Critical," two as "High," six as "Medium," and one "Informational." If successful, a remote threat actor could possibly exploit these vulnerabilities and take control of an affected device or system. Additional information on the "Critical" and "High" vulnerabilities are as follows:

- Cisco SD-WAN vManage Unauthenticated REST API Access Vulnerability has a CVSS base score of 9.1 and a "Critical" rating. This vulnerability, tracked as CVE-2023-20214, is due to insufficient request validation when using the REST API feature. If successful, a threat actor could exploit this vulnerability by sending a crafted API request to an affected vManage instance. This would allow the threat actor to be able to receive and send information to the configuration of the affected Cisco vManage instance. According to Cisco, this flaw only affects the REST API and does not affect the web-based management interface or the CLI.
- Cisco AnyConnect Secure Mobility Client Software for Windows and Cisco Secure Client Software for Windows Privilege Escalation Vulnerability has a CVSS base score of 7.8 and a "High" rating. This

vulnerability, tracked as CVE-2023-20178 is due to improper permissions assigned to a temporary directory created during the update process. A threat actor could possibly exploit this vulnerability by abusing a specific function of the Windows installer process. A successful exploit could allow the threat actor to execute code with SYSTEM privileges.

- Cisco ACI Multi-Site CloudSec Encryption Information Disclosure Vulnerability has a CVSS base score of 7.4 and a “High” rating. This vulnerability, tracked as CVE-2023-20185, is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. A threat actor with an on-path position between the ACI sites could exploit this flaw by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit of this vulnerability could allow the threat actor to read or modify the traffic that is transmitted between the sites.

HC3 recommends that users review the above advisories and apply the necessary updates. For a complete list of Cisco security advisories released in July, 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.

Fortinet

Fortinet’s July vulnerability advisory addresses several vulnerabilities across different Fortinet products, including a critical vulnerability (CVE-2023-33308) which is a stacked-based overflow in FortiOS and FortiProxy with a CVSS Score of 9.8. If successful, a remote threat actor can exploit this vulnerability and take control of a compromised device or system. Products affected by this are: FortiOS version 7.2.0 through 7.2.3, FortiOS version 7.0.0 through 7.0.10, FortiProxy version 7.2.0 through 7.2.2, FortiProxy version 7.0.0 through 7.0.9 &nbsp. HC3 recommends all users review Fortinet’s security advisory FG-IR-23-183 and Fortinet’s July 2023 Vulnerability Advisories page for additional information, and apply all necessary updates and patches immediately. For a complete list of vulnerabilities addressed in July, click here to view FortiGuard Labs’ Vulnerability Advisories page.

VMWare

VMWare released security updates addressing two moderate rated vulnerabilities this month. The first update, VMSA-2023-0015, addresses a bypass authentication vulnerability (CVE-2023-20899) in VMware SD-WAN (Edge). A threat actor that gains network access to the Edge Local Web UI could download an Edge Diagnostic bundle of the application without authentication. Local Web UI Access is disabled by default. The second update, VMSA-2023-0016, addresses an information disclosure vulnerability (CVE-2023-20891) due to the logging of credentials in hex encoding in platform system audit logs that impacts VMWare Tanzu Application Service for VMs and Isolation Segment. A threat actor who can gain access to the platform system audit logs can access hex encoded CF API admin credentials and will have the ability to push new malicious versions of an application. In a default deployment, non-admin users do not have access to the platform system audit logs. To remediate these vulnerabilities, apply the updates listed in the 'Fixed Version' column of the 'Response Matrix' for VMSA-2023-0015 and VMSA-2023-0016.

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 immediately apply patches listed in the 'Fixed Version' column of the 'Response Matrix' that can be accessed by clicking directly on the security advisory.

MOVEit Transfer Critical Vulnerability

MOVEit Transfer software received an update that fixed one critical-severity SQL injection bug and two other less severe vulnerabilities. MOVEit is a managed file transfer software that encrypts files and uses secure File Transfer Protocols to transfer data with automation, analytics, and failover options. Progress, the developer of MOVEit, has released a Service Pack to address these vulnerabilities (CVE-2023-36934, CVE-2023-36932, CVE-2023-36933) in the MOVEit Transfer software. SQL injection vulnerabilities allow threat actors to craft special queries to possibly gain access to a database, or tamper with it by executing code and obtain sensitive information. For cyberattacks of this nature to be possible, the target application must suffer from a lack of appropriate input/output data sanitization. HC3 recommends that all users protect their MOVEit Transfer environment by reviewing Progress Software's MOVEit Transfer Service Pack and applying the necessary product updates immediately.

Oracle

Oracle released its July Critical Patch Update Advisory, Solaris Third Party Bulletin, and Linux Bulletin to address vulnerabilities affecting multiple products. If successful, a remote threat actor can exploit these vulnerabilities to take control of an affected device or system. HC3 recommends all users and administrators follow CISA's guidance, which encourages users and administrators to review Oracle's July 2023 Critical Patch Update Advisory, Solaris Third Party Bulletin, and Linux Bulletin, and apply the necessary updates. For a complete list of Oracle's security and software updates for July, click here. HC3 recommends all users install updates and apply patches immediately.

Adobe

Adobe released two security advisories that addressed 15 vulnerabilities in Adobe InDesign and Adobe ColdFusion. Three of the 15 vulnerabilities are rated as "Critical" severity vulnerabilities and could lead to arbitrary code execution and security feature bypass. HC3 recommends that users review the following Adobe security releases:

- APSB23-38
- APSB23-40
- APSB23-41

If successful, a threat actor can exploit these vulnerabilities and take control of an affected system or device. For a complete list of Adobe security updates, click here. HC3 recommends all users apply necessary updates and patches immediately

References

Adobe Releases Security Updates for ColdFusion
https://www.cisa.gov/news-events/alerts/2023/07/18/adobe-releases-security-updates-coldfusion

Adobe Releases Security Updates for ColdFusion and InDesign
https://www.cisa.gov/news-events/alerts/2023/07/11/adobe-releases-security-updates-coldfusion-and-indesign

Android July security updates fix three actively exploited bugs
https://www.bleepingcomputer.com/news/security/android-july-security-updates-fix-three-actively-exploited-bugs/

Android Security Updates Patch 3 Exploited Vulnerabilities
https://www.securityweek.com/android-security-updates-patches-3-exploited-vulnerabilities/

Apple & Microsoft Patch Tuesday – July 2023 Edition
https://krebsonsecurity.com/2023/07/apple-microsoft-patch-tuesday-july-2023-edition/

Apple Releases Security Updates for Multiple Products
https://www.cisa.gov/news-events/alerts/2023/07/25/apple-releases-security-updates-multiple-products

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

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

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

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

Google finds more Android, iOS zero-days used to install spyware
https://www.bleepingcomputer.com/news/security/google-finds-more-android-ios-zero-days-used-to-install-spyware/

Industrial Spy data extortion market gets into the ransomware game
https://www.bleepingcomputer.com/news/security/industrial-spy-data-extortion-market-gets-into-the-ransomware-game/

July 2023 Microsoft Patch Tuesday
https://isc.sans.edu/diary/July+2023+Microsoft+Patch+Update/30018/

July 2023 Vulnerability Advisories
https://www.fortiguard.com/psirt-monthly-advisory/july-2023-vulnerability-advisories

Microsoft discloses more than 130 vulnerabilities as part of July's Patch Tuesday, four exploited in the wild
https://blog.talosintelligence.com/microsoft-patch-tuesday-july-2023/

Microsoft July 2023 Patch Tuesday warns of 6 zero-days, 132 flaws
https://www.bleepingcomputer.com/news/microsoft/microsoft-july-2023-patch-tuesday-warns-of-6-zero-days-132-flaws/

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

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

Microsoft: Unpatched Office zero-day exploited in NATO summit attacks
https://www.bleepingcomputer.com/news/security/microsoft-unpatched-office-zero-day-exploited-in-nato-summit-attacks/

MOVEit Transfer customers warned to patch new critical flaw
https://www.bleepingcomputer.com/news/security/moveit-transfer-customers-warned-to-patch-new-critical-flaw/

MOVEit Transfer Service Pack (July 2023)
https://community.progress.com/s/article/MOVEit-Transfer-Service-Pack-July-2023

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

Oracle Critical Patch Update Advisory - July 2023
https://www.oracle.com/security-alerts/cpujul2023.html

Oracle Releases Security Updates
https://www.cisa.gov/news-events/alerts/2023/07/18/oracle-releases-security-updates

Patch Tuesday July 2023 Updates – Vulnerability Digest from Action1
https://www.action1.com/patch-tuesday-july-2023/

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

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

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

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