HC3: Monthly Cybersecurity Vulnerability Bulletin
May 16, 2023 TLP:CLEAR Report: 202305161500

April Vulnerabilities of Interest to the Health Sector

In April 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 April are from Microsoft, Google/Android, Apple, Mozilla, SAP, Cisco, Fortinet, VMWare, and Adobe. A vulnerability is given the classification as a zero-day if it is actively exploited with no fix available or 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 17 vulnerabilities in April 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 97 vulnerabilities and one actively exploited zero-day vulnerability in April. Seven of these vulnerabilities have been classified as 'Critical,' which is one of the most severe types of vulnerabilities, as they allow remote code execution. The number of bugs in each vulnerability category is listed as follows:

- 20 Elevation of Privilege Vulnerabilities
- 8 Security Feature Bypass Vulnerabilities
- 45 Remote Code Execution Vulnerabilities
- 10 Information Disclosure Vulnerabilities
- 9 Denial of Service Vulnerabilities
- 6 Spoofing Vulnerabilities

This count does not include seventeen Microsoft Edge vulnerabilities fixed earlier in the month. April's Patch Tuesday addresses one zero-day vulnerability actively exploited in attacks. Tracked as CVE-2023-28252 , this zero-day is a Windows Common Log File System Driver Elevation of Privilege Vulnerability. According to Microsoft's advisory, a threat actor "who successfully exploited this vulnerability could gain SYSTEM privileges." It is also worth noting that Microsoft Office, Word, and Publisher remote code execution vulnerabilities were also addressed in April. These vulnerabilities, tracked as CVE-2023-

28285, CVE-2023-28295, CVE-2023-28287, and CVE-2023-28311, can be exploited simply by opening malicious documents.

For a complete list of Microsoft vulnerabilities released in April 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 released security updates in April for Android devices with fixes for over 65 vulnerabilities, including two critical vulnerabilities that could lead to remote code execution. Every month, security updates are released in two parts: the first part of the update arrived as the 2023-04-01 security patch level, and 26 vulnerabilities were resolved in the Framework and System components. Many of these vulnerabilities are high-severity bugs that lead to information disclosure or elevation of privilege. Two of the 16 issues addressed in the System component are critical-severity RCE vulnerabilities, tracked as CVE-2023-21085 and CVE-2023-21096. The second part of Android's security update arrived on devices as the 2023-04-05 security patch level. This security update included fixes for 40 vulnerabilities in Arm, Kernel, Imagination Technologies, MediaTek, and Qualcomm components. Although most of these vulnerabilities are rated 'high severity', four of these flaws impacting Qualcomm components are rated 'critical severity'.

On April 13, CISA warned of a high severity Android vulnerability that may have been exploited by the Chinese e-commerce app Pinduoduo as a zero-day to spy on its users. Tracked as CVE-2023-20963, this Android Framework security vulnerability allows threat actors to escalate privileges on unpatched Android devices without requiring user interaction. According to CISA, "Android Framework contains an unspecified vulnerability that allows for privilege escalation after updating an app to a higher Target SDK with no additional execution privileges needed." Google addressed this flaw in March with security updates, however according to the vendor, "there are indications that CVE-2023-20963 may be under limited, targeted exploitation." HC3 recommends that 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 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 security 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 could exploit these vulnerabilities and take control of a compromised device or system. 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 15.7.5 and iPadOS 15.7.5
- macOS Monterey 12.6.5
- macOS Big Sur 11.7.6

- Safari 16.4.1
- iOS 16.4.1 and iPadOS 16.4.1
- macOS Ventura 13.3.1

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 for vulnerabilities affecting multiple Mozilla products. If successful, a threat actor could exploit these vulnerabilities and take control of a compromised system. The following security advisories were released:

- Security Vulnerabilities fixed in Firefox 112, Firefox for Android 112, Focus for Android 112 - Mozilla Foundation Security Advisory 2023-13
- Security Vulnerabilities fixed in Firefox ESR 102.10 - Mozilla Foundation Security Advisory 2023-14
- Security Vulnerabilities fixed in Thunderbird 102.10 - Mozilla Foundation Security Advisory 2023-15

HC3 encourages users and administrators to follow CISA's guidance to review Mozilla's security advisories above and apply the necessary updates.

SAP

SAP released security updates for several products, including fixes for two critical-severity vulnerabilities that impact the SAP Diagnostics Agent and the SAP BusinessObjects Business Intelligence Platform. A total of 24 security updates, including five updates to previously issued security notes, were released to address vulnerabilities affecting multiple products. Three of the most critical issues addressed at that time are as follows:

- CVE-2023-27267 (CVSS score: 9.0): This is an insufficient input validation and missing authentication issue impacting the OSCommand Bridge of SAP Diagnostics Agent, version 720, enabling a threat actor to execute scripts on connected agents and fully compromise the system.
- CVE-2023-28765 (CVSS score: 9.8): This is an information disclosure vulnerability impacting SAP BusinessObjects Business Intelligence Platform (Promotion Management), versions 420 and 430, allowing a threat actor with basic privileges to gain access to the lcmbiar file and decrypt it. This would enable the threat actor to access the platform's users' passwords and take over their accounts to perform additional malicious actions.
- CVE-2023-29186 (CVSS score: 8.7): This is a directory traversal flaw impacting SAP NetWeaver versions 707, 737, 747, and 757, allowing a threat actor to upload and overwrite files on the vulnerable SAP server.

For a complete list of SAP's security notes and updates for vulnerabilities released in April, 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 security advisories for vulnerabilities affecting multiple Cisco products, including Industrial Network Director (IND), Modeling Labs, StarOS Software, and BroadbandWorks Network Server. If successful, a remote threat actor could exploit some of these vulnerabilities and take control of a compromised system. HC3 recommends following CISA's guidance that encourages users and administrators to review the following advisories and apply the necessary updates:

- Cisco Secure Network Analytics Remote Code Execution Vulnerability
- Cisco Small Business RV320 and RV325 Dual Gigabit WAN VPN Routers Command Injection Vulnerabilities
- Cisco Evolved Programmable Network Manager, Cisco Identity Services Engine, and Cisco Prime Infrastructure Command Injection Vulnerabilities
- Industrial Network Director
- Cisco Modeling Labs External Authentication Bypass Vulnerability
- Cisco IOS and IOS XE
- StarOS Software Key-Based SSH Authentication Privilege Escalation Vulnerability
- Cisco BroadWorks Network Server TCP Denial of Service Vulnerability

HC3 recommends users and administrators follow CISA's guidance and apply necessary patches immediately. For a complete list of Cisco security advisories released in April, 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 April vulnerability advisory addressed multiple vulnerabilities across different Fortinet products, including FortiOS, FortiGate, FortiClient, FortiNAC, FortiSOAR, FortiDDoS, FortiProxy, FortiWeb, FortiADC, FortiAnalyzer, FortiPresence and FortiManager. Fortinet addressed one critical vulnerability, which is a missing authentication that only affects on-premises servers using FortiPresence. Additional flaws fixed are nine high-level rated vulnerabilities, five medium-level vulnerabilities, and one low-level vulnerability. If successful, a threat actor could exploit one of these vulnerabilities to take control of an affected system. HC3 recommends users follow CISA's guidance, which encourages users and administrators to review Fortinet's April 2023 Vulnerability Advisories page for additional information, and apply all recommended updates and patches immediately. For a complete list of vulnerabilities addressed in April, click here to view FortiGuard Labs' Vulnerability Advisories page.

Adobe

Adobe released security updates addressing numerous vulnerabilities in Adobe software. If successful, a threat actor could exploit these flaws and take control of a compromised system or device. HC3 recommends users follow CISA's guidance, which "encourages users and administrators to review the following Adobe Security Bulletins" for the following products:

- Digital Editions - APSB23-04

- InCopy - APSB23-13
- Acrobat and Reader - APSB23-24
- Substance 3D Stager - APSB23-26
- Dimension - APSB23-27
- Substance 3D Designer - APSB23-28

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

VMWare

VMware released two "Critical" rated security advisories, VMSA-2023-0007 and VMSA-2023-0008. If successful, a threat actor could exploit these vulnerabilities and take control of a compromised device or system. Additional information are as follows:

- VMSA-2023-0007 - This security advisory has a maximum CVSSv3 score of 9.8 and impacts VMware Aria Operations for Logs (formerly vRealize Log Insight). This advisory addresses the following vulnerabilities: CVE-2023-20864, CVE-2023-20865.
- VMSA-2023-0008 - This security advisory has a maximum CVSSv3 score of 9.0 and impacts VMware Workstation Pro / Player (Workstation) as well as VMware Fusion. This advisory addresses the following vulnerabilities: CVE-2023-20869, CVE-2023-20870, CVE-2023-20871, CVE-2023-20872.

For a complete list of VMWare's security advisories, click here. 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.

References

Adobe Product Security Incident Response Team
https://helpx.adobe.com/security.html

Adobe Releases Security Updates for Multiple Products
https://www.cisa.gov/news-events/alerts/2023/04/11/adobe-releases-security-updates-multiple-products

Android's April 2023 Updates Patch Critical Remote Code Execution Vulnerabilities
https://www.securityweek.com/androids-april-2023-updates-patch-critical-remote-code-execution-vulnerabilities/#:~:text=Google%20this%20week%20announced%20the,remote%20code%20execution%20(RCE).

Android Security Bulletin—April 2023
https://source.android.com/docs/security/bulletin/2023-04-01

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

Android Security Bulletin—April 2023
https://source.android.com/docs/security/bulletin/2023-04-01

Apple Releases Security Updates for Multiple Products
https://www.cisa.gov/news-events/alerts/2023/04/11/apple-releases-security-updates-multiple-products

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

CISA adds Microsoft, Apple bugs to exploited vulnerabilities catalog
https://therecord.media/cisa-adds-microsoft-apple-bugs-to-exploited-list

CISA warns of Android bug exploited by Chinese app to spy on users
https://www.bleepingcomputer.com/news/security/cisa-warns-of-android-bug-exploited-by-chinese-app-to-spy-on-users/

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

Cisco Releases Security Advisories for Multiple Products
https://www.cisa.gov/news-events/alerts/2023/04/07/cisco-releases-security-advisories-multiple-products

Cisco Releases Security Advisories for Multiple Products
https://www.cisa.gov/news-events/alerts/2023/04/21/cisco-releases-security-advisories-multiple-products

FortiGuard Labs: April 2023 Vulnerability Advisories
https://www.fortiguard.com/psirt-monthly-advisory/april-2023-vulnerability-advisories

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

Fortinet Releases April 2023 Vulnerability Advisories
https://www.cisa.gov/news-events/alerts/2023/04/11/fortinet-releases-april-2023-vulnerability-advisories

Google, CISA Warn of Android Flaw After Reports of Chinese App Zero-Day Exploitation
https://www.securityweek.com/google-cisa-warn-of-android-flaw-after-reports-of-chinese-app-zero-day-exploitation/

Microsoft (& Apple) Patch Tuesday, April 2023 Edition
https://krebsonsecurity.com/2023/04/microsoft-apple-patch-tuesday-april-2023-edition/

Microsoft and Adobe Patch Tuesday April 2023 Security Update Review
https://blog.qualys.com/vulnerabilities-threat-research/patch-tuesday/2023/04/11/microsoft-and-adobe-patch-tuesday-april-2023-security-update-review

Microsoft, Fortinet, HashiCorp and Other Vendors' April Patches Address Critical and High-Level Vulnerabilities
https://securityboulevard.com/2023/04/microsoft-fortinet-hashicorp-and-other-vendors-april-patches-address-critical-and-high-level-vulnerabilities/

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

Microsoft April 2023 Patch Tuesday
https://isc.sans.edu/diary/Microsoft+April+2023+Patch+Tuesday/29736/

Microsoft April 2023 Patch Tuesday fixes 1 zero-day, 97 flaws
https://www.bleepingcomputer.com/news/microsoft/microsoft-april-2023-patch-tuesday-fixes-1-zero-day-97-flaws/

Mozilla Releases Security Advisories for Multiple Products
https://www.cisa.gov/news-events/alerts/2023/04/11/mozilla-releases-security-advisories-multiple-products

Microsoft Security Response Center April 2023
https://msrc.microsoft.com/blog/2023/04/

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

SAP releases security updates for two critical-severity flaws
https://www.bleepingcomputer.com/news/security/sap-releases-security-updates-for-two-critical-severity-flaws/

SAP Security Patch Day – April 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

Severe Android and Novi Survey Vulnerabilities Under Active Exploitation
https://thehackernews.com/2023/04/severe-android-and-novi-survey.html

The April 2023 Security Update Review
https://www.zerodayinitiative.com/blog/2023/4/11/the-april-2023-security-update-review

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

VMWare Advisory ID: VMSA-2023-0007
https://www.vmware.com/security/advisories/VMSA-2023-0007.html

VMWare Advisory ID: VMSA-2023-0008
https://www.vmware.com/security/advisories/VMSA-2023-0008.html

VMware Releases Security Update for Aria Operations for Logs
https://www.cisa.gov/news-events/alerts/2023/04/21/vmware-releases-security-update-aria-operations-logs

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