HC3: Monthly Cybersecurity Vulnerability Bulletin
July 13, 2023 TLP:CLEAR Report: 202307131000

June Vulnerabilities of Interest to the Health Sector

In June 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 June are from Microsoft, Google/Android, Apple, Mozilla, SAP, Cisco, Fortinet, VMWare, and MOVEit. 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 24 vulnerabilities in June 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 78 vulnerabilities, including 38 remote code execution flaws in June. While all 38 remote code execution vulnerabilities were fixed, Microsoft only listed six vulnerabilities as 'Critical,' including denial of service attacks, remote code execution, and privilege elevation. The number of bugs in each vulnerability category is listed as follows:

- 17 Elevation of Privilege Vulnerabilities
- 3 Security Feature Bypass Vulnerabilities
- 32 Remote Code Execution Vulnerabilities
- 5 Information Disclosure Vulnerabilities
- 10 Denial of Service Vulnerabilities
- 10 Spoofing Vulnerabilities
- 1 Edge - Chromium Vulnerabilities

The list above does not include 16 Microsoft Edge vulnerabilities fixed on June 2nd. There were no zero-day vulnerabilities or actively exploited flaws this month. Some notable vulnerabilities are as follows:

- CVE-2023-29357 – This is a Microsoft SharePoint Server Elevation of Privilege Vulnerability with a CVSS score of 8.5. Microsoft has addressed this privilege elevation vulnerability in Microsoft

SharePoint that could provide threat actors the ability to assume the privileges of other users, including administrators. According to Microsoft's advisory, "An attacker who has gained access to spoofed JWT authentication tokens can use them to execute a network attack which bypasses authentication and allows them to gain access to the privileges of an authenticated user."

- CVE-2023-32031 – This is a Microsoft Exchange Server Remote Code Execution Vulnerability with a CVSS score of 8.8. Microsoft has fixed this Microsoft Exchange vulnerability that could allow authenticated, remote code execution. According to Microsoft's advisory, "The attacker for this vulnerability could target the server accounts in an arbitrary or remote code execution. As an authenticated user, the attacker could attempt to trigger malicious code in the context of the server's account through a network call."

For a complete list of Microsoft vulnerabilities released in June and their ratings, 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 June for Android devices with fixes for over 50 vulnerabilities, including an Arm Mali GPU Kernel Driver flaw exploited by spyware vendors, which Google reported in March 2023. Tracked as CVE-2022-22706 , the exploited vulnerability is a kernel driver issue that allows a non-privileged user to achieve write access to read-only memory pages. This flaw has been used in targeted attacks and was fixed by Arm in January 2022.

Every month, security updates are released in two parts. The first part of the update arrived as the 2023-06-01 security patch level, which resolved 10 vulnerabilities in the Framework component and 13 flaws in the System component. Three of the addressed vulnerabilities are rated "Critical severity" remote code execution (RCE) flaws, tracked as CVE-2023-21127, CVE-2023-21108, and CVE-2023-21130. According to Android's Security Bulletin, "The most severe of these issues is a critical security vulnerability in the System component that could lead to remote code execution over Bluetooth, if HFP support is enabled, with no additional execution privileges needed. User interaction is not needed for exploitation." The remaining 20 vulnerabilities are rated "High Severity" and can lead to denial-of-service (DoS), escalation of privilege, or information disclosure. The second part of Android's security update arrived on devices as the 2023-06-05 security patch level. This security update fixes 33 flaws in Arm (3 vulnerabilities), Imagination Technologies (2), Unisoc (4), Widevine DRM (2), and Qualcomm components (22).

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 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 and administrators follow CISA's guidance, which encourages users and administrators to review the following advisories and apply the necessary updates:

- watchOS 8.8.1
- macOS Big Sur 11.7.8
- macOS Monterey 12.6.7
- iOS 15.7.7 and iPadOS 15.7.7
- watchOS 9.5.2
- macOS Ventura 13.4.1
- iOS 16.5.1 and iPadOS 16.5.1

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, including Firefox 114 and Firefox ESR 102.12. 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:

- Firefox 114
- Firefox ESR 102.12

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 13 new security notes to address vulnerabilities affecting multiple products. If successful with launching an attack, a threat actor could exploit these vulnerabilities and take control of a compromised device or system. This month, there were four vulnerabilities rated as "High", eight rated as "Medium," and one rated as "Low" in severity. A breakdown of security notes for vulnerabilities with a "High" severity rating are as follows:

- **Security Note #3102769** (CVE-2021-42063) has a CVSS score of 8.8 and a "High" severity rating. This is an update to a security note for the Cross-Site Scripting (XSS) vulnerability in SAP Knowledge Warehouse released during the December 2021 Patch Tuesday. Product(s) impacted: SAP Knowledge Warehouse, Versions-7.30, 7.31,7.40,7.50.
- **Security Note #3324285** (CVE-2023-33991) has a CVSS score of 8.2 and a "High" severity rating. This is a Stored Cross-Site Scripting (Stored XSS) vulnerability in UI5 Variant Management. Product(s) impacted: SAP UI5 Variant Management, Versions– SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, UI_700 200.

- **Security Note# 3301942** (CVE-2023-2827) has a CVSS score of 7.9 and a "High" severity rating. This vulnerability is a Missing Authentication in SAP Plant Connectivity and Production Connector for SAP Digital Manufacturing. Product(s) impacted: SAP Plant Connectivity, Version – 1.
- **Security Note#3326210** (CVE-2023-30743) has a CVSS score of 7.1 , a "High" severity rating , and is an update to a Security Note released on May 2023 Patch Day. This vulnerability is an Improper Neutralization of Input in SAPUI5. Product(s) impacted: -SAPUI5, Versions –SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, UI_700 200.

For a complete list of SAP's security notes and updates for vulnerabilities released in June, 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. One advisory was rated "Critical," three were rated as "High," and seven were rated as "Medium." If successful, a remote threat actor could possibly exploit these vulnerabilities and take control of an affected device or system. HC3 recommends users follow CISA's guidance, which encourages users and administrators to review the following advisories and apply the necessary updates:

- Cisco AnyConnect Secure Mobility Client Software for Windows and Cisco Secure Client Software for Windows Privilege Escalation Vulnerability has a CVSS score of 7.8. This vulnerability exists because of improper permissions assigned to a temporary directory that is created during the update process. If successful, a threat actor could 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. CVE-2023-20178 is the vulnerability for this advisory.
- Cisco Expressway Series and Cisco TelePresence Video Communication Server Privilege Escalation Vulnerabilities has a CVSS score of 9.6. These vulnerabilities could allow an authenticated threat actor with Administrator-level read-only credentials to elevate their privileges to Administrator with read-write credentials on a compromised device or system. Vulnerabilities for this advisory are: CVE-2023-20105 and CVE-2023-20192.
- Cisco Unified Communications Manager IM & Presence Service Denial of Service Vulnerability has a CVSS score of 7.5. This vulnerability is due to improper validation of user-supplied input. If successful, a threat actor could exploit this vulnerability by sending a crafted login message to a compromised device. A successful exploit could allow the threat actor to cause an unexpected restart of the authentication service, preventing new users from successfully authenticating. It is important to note that exploitation of this flaw does not impact Cisco Unified CM IM&P users who were authenticated prior to an attack. At this time there are no workarounds that address this vulnerability however, Cisco has released software updates that address this vulnerability which can be accessed by clicking here. CVE-2023-20108 is the vulnerability for this advisory.
- Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software for Firepower 2100 Series Appliances SSL/TLS Denial of Service Vulnerability has a CVSS score of 8.6. This vulnerability is due to an implementation error within the cryptographic functions for SSL/TLS traffic processing when they are offloaded to the hardware. A threat actor could exploit

this vulnerability by sending a crafted stream of SSL/TLS traffic to an affected device. A successful exploit could lead to the threat actor causing an unexpected error in the hardware-based cryptography engine, which could cause the device to reload. At this time there are no workarounds that address this vulnerability however, Cisco has released software updates that address this vulnerability which can be accessed by clicking here. CVE-2023-20006 is the vulnerability for this advisory.

- Cisco AnyConnect Secure Mobility Client Software for Windows and Cisco Secure Client Software for Windows Privilege Escalation Vulnerability has a CVSS score of 7.8. This vulnerability exists because improper permissions are assigned to a temporary directory that is created during the update process. A threat actor could 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. At this time there are no workarounds that address this vulnerability however, Cisco has released software updates that address this vulnerability which can be accessed by clicking here. CVE-2023-20178 is the vulnerability for this advisory.
- Cisco Small Business 200, 300, and 500 Series Switches Web-Based Management Stored Cross-Site Scripting Vulnerability has a CVSS score of 4.8. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by persuading a user of an affected interface to view a page containing malicious HTML or script content. A successful exploit could allow a threat actor to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the threat actor would need to have valid credentials to access the web-based management interface of the affected device. At this time there are no workarounds that address this vulnerability however, Cisco has released software updates that address this vulnerability which can be accessed by clicking here. CVE-2023-20188 is the vulnerability for this advisory.
- Cisco Unified Communications Manager Denial of Service Vulnerability has a CVSS score of 6.8. This flaw is due to insufficient validation of user-supplied input to the web UI of the Self Care Portal. A threat actor could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the threat actor to cause a DoS condition on the affected device. CVE-2023-20116 is the vulnerability for this advisory.
- Cisco Secure Workload Authenticated OpenAPI Privilege Escalation Vulnerability has a CVSS score of 4.3. This vulnerability is due to improper role-based access control (RBAC) of certain OpenAPI operations. A threat actor could exploit this flaw by issuing a crafted OpenAPI function call with valid credentials. A successful exploit could allow a threat actor to execute OpenAPI operations that are reserved for the Administrator user, including the creation and deletion of user labels. CVE-2023-20136 is the vulnerability for this advisory.

Currently there are no workarounds to address these vulnerabilities. For a complete list of Cisco security advisories released in June, 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 June vulnerability advisory addressed several vulnerabilities across different Fortinet products, including a heap-based buffer overflow vulnerability tracked as FG-IR-23-097(CVE-2023-27997) in FortiOS

and FortiProxy. If successful, a threat actor could exploit this vulnerability to take control of a compromised system. According to Fortinet, the vendor is "not linking FG-IR-23-097 to the Volt Typhoon campaign, however Fortinet expects all threat actors, including those behind the Volt Typhoon campaign, to continue to exploit unpatched vulnerabilities in widely used software." HC3 recommends all users review Fortinet's security advisory FG-IR-23-097, Analysis of CVE-2023-27997 and Clarifications on Volt Typhoon Campaign, Fortinet's June 2023 Vulnerability Advisories page for additional information, and apply all necessary updates and patches immediately. For a complete list of vulnerabilities addressed in June, click here to view FortiGuard Labs' Vulnerability Advisories page.

VMWare

VMWare released security updates addressing vulnerabilities in Aria Operations for Networks (Formerly vRealize Network Insight). The vulnerabilities fall within the critical severity range, as a malicious threat actor with network access could possibly perform a command injection attack leading to remote code execution. VMware also released a security update to address multiple memory corruption vulnerabilities in vCenter Server and Cloud Foundation. If successful, a threat actor could exploit these vulnerabilities to take control of a compromised device or system. HC3 recommends users follow CISA's guidance, which encourages users and administrators to review the following VMware Security Advisories and apply the necessary updates:

- VMSA-2023-0012 - VMware Aria Operations for Networks updates address multiple vulnerabilities (CVE-2023-20887, CVE-2023-20888, CVE-2023-20889)
- VMSA-2023-0014 - VMware vCenter Server updates address multiple memory corruption vulnerabilities. (CVE-2023-20892, CVE-2023-20893, CVE-2023-20894, CVE-2023-20895, CVE-2023-20896)

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

A critical vulnerability was discovered in Progress/IPswitch's MOVEit Transfer software. 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. Tracked as CVE-2023-35708, this critical vulnerability could lead to escalated privileges and potential unauthorized access to the environment. This SQL injection vulnerability has been identified in the MOVEit Transfer web application that could allow an un-authenticated threat actor to gain unauthorized access to the MOVEit Transfer database. This impacts Progress MOVEit Transfer versions released before 2021.0.8 (13.0.8), 2021.1.6 (13.1.6), 2022.0.6 (14.0.6), 2022.1.7 (14.1.7), 2023.0.3 (15.0.3). If successful a threat could exploit this flaw and submit a crafted payload to a MOVEit Transfer application endpoint which could possibly result in modification and disclosure of MOVEit database content. HC3 recommends that all MOVEit Transfer software users protect their MOVEit Transfer environment by taking immediate action and following Progress' remediation guidance, which can be viewed by clicking here.

References

Android's June 2023 Security Update Patches Exploited Arm GPU Vulnerability

https://www.securityweek.com/androids-june-2023-security-update-patches-exploited-arm-gpu-vulnerability/

Android's June 2023 Security Update Patches Exploited Arm GPU Vulnerability
https://www.securityweek.com/androids-june-2023-security-update-patches-exploited-arm-gpu-vulnerability/

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

Apple Releases Security Updates for Multiple Products
https://www.cisa.gov/news-events/alerts/2023/06/22/apple-releases-security-updates-multiple-products

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

CISA Adds Five Known Exploited Vulnerabilities to Catalog
https://www.cisa.gov/news-events/alerts/2023/06/23/cisa-adds-five-known-exploited-vulnerabilities-catalog

Cisco Releases Security Advisories for Multiple Products
https://www.cisa.gov/news-events/alerts/2023/06/13/cisco-releases-security-advisories-multiple-products

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

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

Fortinet Releases June 2023 Vulnerability Advisories
https://www.cisa.gov/news-events/alerts/2023/06/13/fortinet-releases-june-2023-vulnerability-advisories

Fortinet Releases Security Updates for FortiOS and FortiProxy
https://www.cisa.gov/news-events/alerts/2023/06/12/fortinet-releases-security-updates-fortios-and-fortiproxy

Google Chrome Releases
https://chromereleases.googleblog.com/

June 2023 Microsoft Patch Tuesday
https://isc.sans.edu/diary/June+2023+Microsoft+Patch+Tuesday/29942

June 2023 Vulnerability Advisories

https://www.fortiguard.com/psirt-monthly-advisory/june-2023-vulnerability-advisories

Microsoft and Adobe Patch Tuesday, June 2023 Security Update Review
https://blog.qualys.com/vulnerabilities-threat-research/2023/06/13/microsoft-patch-tuesday-june-2023-security-update-review

Microsoft's June 2023 Patch Tuesday Addresses 70 CVEs (CVE-2023-29357)
https://www.tenable.com/blog/microsofts-june-2023-patch-tuesday-addresses-70-cves-cve-2023-29357

Microsoft June 2023 Patch Tuesday fixes 78 flaws, 38 RCE bugs
https://www.bleepingcomputer.com/news/microsoft/microsoft-june-2023-patch-tuesday-fixes-78-flaws-38-rce-bugs/

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

Microsoft Patch Tuesday, June 2023 Edition
https://krebsonsecurity.com/2023/06/microsoft-patch-tuesday-june-2023-edition/

Microsoft Releases Updates to Patch Critical Flaws in Windows and Other Software
https://thehackernews.com/2023/06/microsoft-releases-updates-to-patch.html

Microsoft Security Response Center June 2023
https://msrc.microsoft.com/blog/2023/06/

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

MOVEit Transfer Critical Vulnerability – CVE-2023-35708 (June 15, 2023)
https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-15June2023

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

Mozilla Releases Security Updates for Multiple Products
https://www.cisa.gov/news-events/alerts/2023/06/07/mozilla-releases-security-updates-multiple-products

Patch Tuesday – June 2023
https://www.rapid7.com/blog/post/2023/06/13/patch-tuesday-june-2023/

SAP Patches High-Severity Vulnerabilities with June 2023 Security Updates
https://www.securityweek.com/sap-patches-high-severity-vulnerabilities-with-june-2023-security-updates/

SAP Security Notes

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

SAP Security Patch Day June 2023
https://securityboulevard.com/2023/06/sap-security-patch-day-june-2023/

VMware Releases Security Update for Aria Operations for Networks
https://www.cisa.gov/news-events/alerts/2023/06/08/vmware-releases-security-update-aria-operations-networks

VMware Releases Security Update for vCenter Server and Cloud Foundation
https://www.cisa.gov/news-events/alerts/2023/06/23/vmware-releases-security-update-vcenter-server-and-cloud-foundation

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