HC3: Monthly Cybersecurity Vulnerability Bulletin
September 20, 2023 TLP:CLEAR Report: 202309201200

August Vulnerabilities of Interest to the Health Sector

In August 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 August are from Microsoft, Google/Android, Cisco, Apple, Mozilla, 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 given 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 eight vulnerabilities in August 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 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 for 87 flaws, including two actively exploited and twenty-three remote code execution vulnerabilities. While twenty-three RCE bugs were fixed in August, only six were rated as 'Critical.' The number of bugs in each vulnerability category is listed as follows:

- 18 Elevation of Privilege vulnerabilities
- 3 Security Feature Bypass vulnerabilities
- 23 Remote Code Execution vulnerabilities
- 10 Information Disclosure vulnerabilities
- 8 Denial of Service vulnerabilities
- 12 Spoofing vulnerabilities

This count does not include twelve Microsoft Edge (Chromium) vulnerabilities fixed earlier in August. This month's Patch Tuesday addressed two zero-day vulnerabilities, with both exploited in attacks and one of them publicly disclosed. Additional information on the two actively exploited zero-day is as follows:

- CVE-2023-36884 (Microsoft Office Defense in Depth Update - ADV230003) - Microsoft released an Office Defense in Depth update to fix a patch bypass of the previously mitigated and actively

exploited CVE-2023-36884 remote code execution flaw. If successful, this vulnerability allows threat actors to create specially crafted Microsoft Office documents that could bypass the Mark of the Web (MoTW) security feature, causing files to be opened without displaying a security warning and perform remote code execution.

- CVE-2023-38180 - Microsoft has also fixed this actively exploited vulnerability that can lead to a Denial-of-Service (DoS) attack on .NET applications and Visual Studio.

For a complete list of Microsoft vulnerabilities released in August 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 security updates for August include the release of the Chrome 115 update, which addressed 17 security vulnerabilities in the browser. Of the 17 flaws fixed, three are serious type confusion bugs discovered in the V8 JavaScript, tracked as CVE-2023-4068 and CVE-2023-4070, and WebAssembly engine, tracked as CVE-2023-4069. In addition to the V8 and WebAssembly bugs, the August update resolves six other serious vulnerabilities. The most severe of these is CVE-2023-4071, which involves a heap buffer overflow bug in Visuals. This update also addresses an out-of-memory read and write issue in WebGL (CVE-2023-4072), along with an out-of-abstraction-level memory access vulnerability in the ANGLE graphics engine (CVE-2023-4073). Additionally, this update addresses three high-severity vulnerabilities reported externally, which are related to use-after-free issues in Blink, Cast, and WebRTC task scheduling. This month's Chrome version also fixes two moderate vulnerabilities related to extensions. Users can access the update as version 115.0.5790.170 for Mac and Linux and 115.0.5790.170/.171 for Windows. 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.

Cisco

Cisco released security updates to address vulnerabilities in multiple products. If successful, a cyber threat actor can exploit some of these vulnerabilities to take control of an affected system or cause a denial-of service condition. HC3 recommends users follow CISA's guidance, which encourages users and administrators to review the following advisories:

- ThousandEyes Enterprise Agent
- Duo Device Health Application
- Unified CM
- ClamAV HFS+
- ClamAV

HC3 recommends that users apply the necessary patches and updates immediately. For a complete list of Cisco security advisories released in August, 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.

Apple

Apple released security updates to address vulnerabilities in multiple products and acted quickly in addressing a new zero-day vulnerability that has been exploited in Advanced Persistent Threat (APT) attacks. The flaw discovered in the iOS and macOS kernel is a serious risk to iOS, iPadOS, and macOS devices. This vulnerability, tracked as CVE-2023-38606, has been actively exploited in attacks against devices running versions prior to iOS 15.7.1. Apple has released security updates for iOS, macOS, and iPadOS platforms to address this critical issue. According to researchers, CVE-2023-38606 was part of a zero-click exploit chain that was utilized to deploy Triangulation spyware on iPhones via iMessage exploits. CVE-2023-37450,a previous WebKit vulnerability, which had been exploited earlier, was patched in a Rapid Security Response (RSR). If successful, a remote threat actor could leverage these vulnerabilities on compromised devices to manipulate crucial kernel states. To mitigate these risks, Apple has improved checks and state management in its updates. The recent security updates from Apple address at least 25 documented security bugs on iPhones and iPads, including several issues that could potentially expose mobile devices to Remote Code Execution (RCE) attacks. Among the vulnerabilities fixed is CVE-2023-32409 in tvOS 16.6 and watchOS 9.6. Apple has also addressed security issues in the Safari browser with Safari 16.6 and has provided updates for older versions of the iPhone and iPad (iOS 15.7.8 and iPadOS 15.7.8), as well as macOS Ventura 13.5. devices.

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

Mozilla

Mozilla released security advisories in August addressing vulnerabilities affecting multiple Mozilla products, including Firefox 116, Firefox ESR 115.1, Firefox ESR 102.14, Thunderbird 115.1, and Thunderbird 102.14, Firefox 117, Firefox ESR 115.2, Firefox ESR 102.15, Thunderbird 115.2, and Thunderbird 102.15. 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 116
- Firefox ESR 115.1
- Firefox ESR 102.14
- Thunderbird 115.1
- Thunderbird 102.14
- Firefox 117
- Firefox ESR 115.2
- Firefox ESR 102.15

- Thunderbird 115.2
- Thunderbird 102.15

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.

Fortinet

Fortinet's August Vulnerability Advisory addresses several vulnerabilities across different Fortinet products, including a critical vulnerability (CVE-2023-29182). A stack-based buffer overflow vulnerability [CWE- 121] in Fortinet FortiOS before 7.0.3 allows a privileged attacker to execute arbitrary code via specially crafted CLI commands, provided the attacker were able to evade FortiOS stack protections. If successful, a remote threat actor can exploit this vulnerability and take control of a compromised device or system. HC3 recommends all users review Fortinet's security advisory FG-IR-23-149 and Fortinet's August 2023 Vulnerability Advisories page for additional information, and apply all necessary updates and patches immediately. For a complete list of vulnerabilities addressed in August, click here to view FortiGuard Labs' Vulnerability Advisories page.

VMWare

VMWare released security updates addressing multiple vulnerabilities in VMware's Workspace ONE Access, Access Connector, Identity Manager, Identity Manager Connector, and vRealize Automation. A remote attacker could exploit some of these vulnerabilities to take control of an affected system. According to VMware, the vendor "has confirmed malicious code that can exploit CVE-2022-31656 and CVE-2022-31659 in impacted products." To remediate these vulnerabilities, apply the updates listed in the 'Fixed Version' column of the 'Response Matrix' for VMware Security Advisory VMSA-2022-0021.

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', which 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 users review the following Adobe security releases:

- Adobe Acrobat and Reader: APSB23-30
- Adobe Commerce: APSB23-42
- Adobe Dimension: APSB23-44
- Adobe XMP Toolkit SDK: APSB23-45

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 Multiple Products
https://www.cisa.gov/news-events/alerts/2023/08/08/adobe-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

Cisco Releases Security Advisories for Multiple Products
https://www.cisa.gov/news-events/alerts/2023/08/17/cisco-releases-security-advisories-multiple-products

Microsoft August 2023 Patch Tuesday warns of 2 zero-days, 87 flaws
https://www.bleepingcomputer.com/news/microsoft/microsoft-august-2023-patch-tuesday-warns-of-2-zero-days-87-flaws/

Microsoft Office Defense in Depth Update
https://msrc.microsoft.com/update-guide/vulnerability/ADV230003

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

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/

Mozilla Releases Security Updates for Multiple Products
https://www.cisa.gov/news-events/alerts/2023/08/30/mozilla-releases-security-updates-multiple-products

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

SANS Internet Storm Center: Microsoft August 2023 Patch Tuesday
https://isc.sans.edu/diary/Microsoft+August+2023+Patch+Tuesday/30106/

VMware Releases Security Updates
https://www.cisa.gov/news-events/alerts/2022/08/03/vmware-releases-security-updates

VMware Releases Security Updates
https://www.cisa.gov/news-events/alerts/2022/08/03/vmware-releases-security-updates

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