HC3: Monthly Cybersecurity Vulnerability Bulletin
September 6, 2022 TLP: White Report: 202209061200

August Vulnerabilities of Interest to the Health Sector

In August 2022, 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 this month are from Microsoft, Google/Android, Apple, Cisco, Adobe, Intel, SAP, and VMWare. 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 23 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 the US 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

This month Microsoft released fixes for 121 vulnerabilities in its Windows operating systems and related software including the actively exploited 'DogWalk' zero-day vulnerability. Seventeen vulnerabilities addressed are classified as 'Critical' and they allow remote code execution or elevation of privileges.

The number of bugs in each vulnerability category is listed as follows:

- 64 Elevation of Privilege Vulnerabilities
- 6 Security Feature Bypass Vulnerabilities
- 31 Remote Code Execution Vulnerabilities
- 12 Information Disclosure Vulnerabilities
- 7 Denial of Service Vulnerabilities
- 1 Spoofing Vulnerability

Twenty vulnerabilities previously fixed in Microsoft Edge are not included in this count. In addition, this month's Patch Tuesday addressed two zero-day vulnerabilities, with one listed as actively exploited. Some noteworthy vulnerabilities are as follows:

- CVE-2022-34713 also referred to as 'DogWalk' is the actively exploited zero-day vulnerability addressed this month. It is a Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability.'

- CVE-2022-30134 is the other zero-day vulnerability and it is a Microsoft Exchange Information Disclosure Vulnerability that gives a threat actor the ability to read email messages from a target's device.

To view the complete list of Microsoft vulnerabilities released in August and their rating click here and for all security updates click here. HC3 recommends patching and testing immediately as all vulnerabilities can adversely impact the health sector.

Google/Android

For the month of August, Google released the latest security updates for the Chrome browser which upgrades the Chrome browser's build as well as addresses 27 vulnerability fixes and security threats.

This update in Google's Chrome browser moves the four-part version number to 104.0.5112.101 (Mac and Linux), or to 104.0.5112.102 (Windows).

According to Google, the new version addresses 11 security fixes, including one with the remark "an exploit [for this vulnerability] exists in the wild" which is essentially makes it a zero-day. In addition, Google's release bulletin mentions the following noteworthy vulnerabilities:

- CVE-2022-2852: Use after free in FedCM.
- CVE-2022-2854: Use after free in SwiftShader.
- CVE-2022-2855: Use after free in ANGLE.
- CVE-2022-2857: Use after free in Blink.
- CVE-2022-2858: Use after free in Sign-In Flow.
- CVE-2022-2853: Heap buffer overflow in Downloads.
- CVE-2022-2856: Insufficient validation of untrusted input in Intents. (Zero-day.)
- CVE-2022-2859: Use after free in Chrome OS Shell.
- CVE-2022-2860: Insufficient policy enforcement in Cookies.
- CVE-2022-2861: Inappropriate implementation in Extensions API.

HC3 recommends that users refer to the Android and Google Play Protect mitigations section for details on the Android security platform protections and Google Play Protect, which improve the security of the Android platform. In addition to this, users should review Google's Stable Channel Update for Desktop for more information related to this update. 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. A summary of the mitigations provided by the Android security platform and service protections can be viewed by clicking here.

Apple

For the month of August, Apple released security updates to address vulnerabilities in iOS and iPadOS, macOS Monterey, and Safari. If successful, a threat actor could exploit one of these vulnerabilities and take control of compromised device. HC3 recommends following CISA's guidance that encourages all users and administrators to review the Apple security updates page for the following products and apply the necessary updates as soon as possible:

- MacOS Monterey 12.5.1
- iOS 15.6.1 and iPadOS 15.6.1

- Safari 15.6.1

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

Cisco

Cisco released 16 security updates this month for vulnerabilities affecting ACI Multi-Site Orchestrator, FXOS, and NX-OS software. If successful with their attack, a threat actor could exploit some of these vulnerabilities and take control of their target's device. HC3 recommends followings CISA's guidance which encourages users and administrators to review advisories for ACI Multi-Site Orchestrator, FXOS, and NX-OS and apply the necessary updates.

For a complete list of Cisco security advisories released, 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. HC3 recommends users and administrators follow CISA's guidance and apply necessary patches immediately.

Adobe

This month Adobe released 5 advisories with updates to address 25 vulnerabilities affecting Adobe Acrobat and Reader, Commerce, FrameMaker, Illustrator, and Adobe Premiere Elements applications. Of these 25 vulnerabilities, 15 are rated as Critical; ranging in severity from a CVSS score of 7.8/10 to 9.1/10. Additional information for each is as follows:

The update for Acrobat and Reader addresses three Critical-rated and four Important-rated vulnerabilities. If a threat actor can lure or convince a user to open a specially crafted file the critical vulnerabilities could allow code execution. Commerce had seven total fixes including four Critical-rated bugs. Two of these vulnerabilities could allow code execution and two could also lead to a privilege escalation. With a CVSS of 9.1, the XML injection vulnerability fixed by highest CVSS of Adobe's release. The patch for Illustrator contains two Critical and two Important fixes for vulnerabilities, the most severe could lead to code execution if specially crafted file is opened. Six FrameMaker flaws, five of which could lead to code execution were also discovered. There is also a single Critical-rated CVE in the Premier Elements patch caused by an uncontrolled search path element. At the time of release, none of the vulnerabilities addressed by Adobe in August are listed as publicly known or under active attack. Adobe categorizes the most of these updates as a deployment priority rating of 3, with the Acrobat patch being the lone exception at 2. HC3 recommends applying the appropriate security updates and patches that can be found on Adobe's Product Security Incident Response Team (PSIRT) by clicking here.

Intel

Intel issued four security center advisories for their products this month. These advisories provide fixes or workarounds for vulnerabilities that are identified with Intel products. The following vulnerabilities with a high severity rating were addressed:

- INTEL-SA-00712 Intel NUC Laptop Kit Advisory -Potential security vulnerabilities in some Intel NUC Laptop Kits could allow escalation of privilege. Intel is releasing firmware updates to mitigate these potential vulnerabilities. Details on vulnerabilities with a high severity rating and their hyperlinks

are as follows: (CVE-2022-28858 , CVE-2022-33209 8.2 CVSS score; CVE-2022-27493 , CVE-2022-34488 7.5 CVSS score) - Improper buffer restriction in the firmware for some Intel(R) NUC Laptop Kits before version BC0076 may allow a privileged user to potentially enable escalation of privilege via local access.

- INTEL-SA-00709 Intel AMT and Intel Standard Manageability Advisory - Potential security vulnerabilities in the Intel Active Management Technology (AMT) and Intel Standard Manageability may allow escalation of privilege or information disclosure. Intel is releasing prescriptive guidance to mitigate these potential vulnerabilities. (CVE-2022-30601 8.2 CVSS score) - Insufficiently protected credentials for Intel(R) AMT and Intel(R) Standard Manageability may allow an unauthenticated user to potentially enable information disclosure and escalation of privilege via network access. Additional vulnerabilities with high severity ratings and their hyperlinks are as follows: CVE-2022-30944 7.4 CVSS and CVE-2022-28697 7.0 CVSS.

Intel's software security guidance can be viewed by clicking here. HC3 recommends users apply necessary updates and patches immediately.

SAP

This month SAP released 7 security notes or updates to address vulnerabilities affecting multiple products. If successful a threat actor could exploit some of these vulnerabilities to take control of a compromised system. This month there was one vulnerability with severity a rating of "Hot News" which is the most severe rating, however this was an update to a security note released in April 2018. In addition to this, there was one vulnerability with a "High" severity rating and 5 with a "Medium" severity. A breakdown of advisories for vulnerabilities with a "Hot News" and a "High" severity rating are as follows:

- *Security Note#2622660* (10 CVSS Score) - Update to Security Note released on April 2018 Patch Day: Security updates for the browser control Google Chromium delivered with SAP Business Client. Product: SAP Business Client, Versions -6.5, 7.0, 7.70.
- *Security Note#3210823 or CVE-2022-32245* - (8.2 CVSS score) - Information disclosure vulnerability in SAP BusinessObjects Business Intelligence Platform (Open Document) Product: SAP BusinessObjects Business Intelligence Platform (Open Document), Versions -420, 430.

For a complete list of SAP's security notes and updates for vulnerabilities released this month 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.

VMWare

VMWare released five security advisories this month, one with a severity rating of 'Critical', two 'Important,' and three 'Moderate.' Additional information on some of these is as follows:

- VMSA-2022-0021.1 (CVSS 4.7-9.8) has a 'Critical severity rating and impact the following products: VMware Workspace ONE Access (Access), VMware Workspace ONE Access Connector (Access Connector), VMware Identity Manager (vIDM), VMware Identity Manager Connector (vIDM Connector), VMware vRealize Automation (vRA), VMware Cloud Foundation, vRealize Suite Lifecycle Manager. CVE's include: CVE-2022-31656, CVE-2022-31657, CVE-2022-31658, CVE-2022-

31659, CVE-2022-31660, CVE-2022-31661, CVE-2022-31662, CVE-2022-31663, CVE-2022-31664, CVE-2022-31665.

- VMSA-2022-0022 (CVSS 5.6 – 7.2) has an 'Important' rating and includes CVE's CVE-2022-31672, CVE-2022-31673, CVE-2022-31674, CVE-2022-31675. VMware vRealize Operations contains multiple vulnerabilities including an authentication bypass vulnerability that was reported as actively exploited at the time of the advisory's release.

HC3 recommends recommend users follows VMWare's guidance and immediately apply patches listed in the 'Fixed Version' column of the 'Response Matrix' that can be accessed by clicking here.

References

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

Android Security Bulletin – August 2022
https://source.android.com/docs/security/bulletin/2022-08-01

Apple Releases Security Updates for Multiple Products
https://www.cisa.gov/uscert/ncas/current-activity/2022/08/18/apple-releases-security-updates-multiple-products

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

August 2022 Patch Tuesday | Microsoft Releases 121 Vulnerabilities with 17 Critical, plus 20 Microsoft Edge (Chromium-Based); Adobe Releases 5 Advisories, 25 Vulnerabilities with 15 Critical.
https://blog.qualys.com/vulnerabilities-threat-research/2022/08/09/august-2022-patch-tuesday

Chrome browser gets 11 security fixes with 1 zero-day – update now!
https://nakedsecurity.sophos.com/2022/08/17/chrome-browser-gets-11-security-fixes-with-1-zero-day-update-now/

Cisco Releases Security Updates for Multiple Products
https://www.cisa.gov/uscert/ncas/current-activity/2022/08/25/cisco-releases-security-updates-multiple-products

Intel Software Security Guidance
https://www.intel.com/content/www/us/en/developer/topic-technology/software-security-guidance/overview.html

Intel Product Security Center Advisories
https://www.intel.com/content/www/us/en/security-center/default.html

Krebs on Security: Microsoft Patch Tuesday, August 2022
https://krebsonsecurity.com/2022/08/microsoft-patch-tuesday-august-2022-edition/

Microsoft August 2022 Patch Tuesday fixes exploited zero-day, 121 flaws
https://www.bleepingcomputer.com/news/microsoft/microsoft-august-2022-patch-tuesday-fixes-exploited-zero-day-121-flaws/

Microsoft Patch Tuesday, August 2022 Edition
https://krebsonsecurity.com/2022/08/microsoft-patch-tuesday-august-2022-edition/

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

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

Microsoft Security Updates
https://msrc.microsoft.com/update-guide/releaseNote/2022-Aug

Microsoft August 2022 Patch Tuesday fixes exploited zero-day, 121 flaws
https://www.bleepingcomputer.com/news/microsoft/microsoft-august-2022-patch-tuesday-fixes-exploited-zero-day-121-flaws/

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

SAP Security Patch Day – August 2022
https://dam.sap.com/mac/app/e/pdf/preview/embed/ucQrx6G?ltr=a&rc=10

SAP Security Patch Day – August 2022
https://securitybridge.com/sap-patchday/sap-security-patch-day-august-2022/

Stable Channel Update for Desktop
https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_16.html

The August 2022 Security Update Review
https://www.zerodayinitiative.com/blog/2022/8/9/the-august-2022-security-update-review

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