HC3: Monthly Cybersecurity Vulnerability Bulletin
August 15, 2022 TLP: White Report: 202208151700

July Vulnerabilities of Interest to the Health Sector

In July 2022, a number of patches to vulnerabilities that impact the health sector have been released that require attention. This includes the monthly Patch Tuesday items released by several vendors on the second Tuesday of each month, along with mitigation steps and patches. 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 3 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 US federal enterprise.

Vulnerabilities that are entered into this catalog are required to be patched by their associated deadline by all US 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 one actively exploited zero-day vulnerability and 84 flaws addressing CVEs in Microsoft Windows and Windows Components; Windows Azure components; Microsoft Defender for Endpoint; Microsoft Edge (Chromium-based); Office and Office Components; Windows BitLocker; Windows Hyper-V; Skype for Business and Microsoft Lync; Open-Source Software; and Xbox.

Four of the 84 vulnerabilities fixed in this month's update allow remote code execution and are classified as 'Critical' and 80 as 'Important.' The number of bugs in each vulnerability category are as follows:

- 52 Elevation of Privilege Vulnerabilities
- 4 Security Feature Bypass Vulnerabilities
- 12 Remote Code Execution Vulnerabilities
- 11 Information Disclosure Vulnerabilities
- 5 Denial of Service Vulnerabilities

In addition to this, two CVEs were patched in Microsoft Edge (Chromium-based) bringing the number to a total of 87 CVEs. None of the new vulnerabilities addressed in July are listed as publicly known. A few updates of note are as follows:

- CVE-2022-22047 (CVSS 7.8) is a Windows CSRSS Elevation of Privilege. This vulnerability is listed as being under active attack, however at this time there is no information from Microsoft on where this flaw is being exploited. If successful in launching an attack, this vulnerability allows a threat actor the ability to execute code as SYSTEM, provided they can execute other code on the target.

Flaws of this nature are usually paired with a code execution bug, often a specially crafted Office or Adobe document, to take over a system; attacks of this nature often rely on macros.

- CVE-2022-30216 (CVSS 8.8) is a Windows Server Service Tampering Vulnerability. This patch addresses a tampering vulnerability in the Windows Server Service that could allow an authenticated threat actor to upload a malicious certificate to a target server. While this is listed as "Tampering," a threat actor could install their own certificate on a target system and use this vulnerability for code execution or other malicious activity. Microsoft does give this its highest exploit index rating which means they expect active exploits within 30 days. HC3 recommends testing and patching immediately, particularly on critical servers.

- CVE-2022-22029 (CVSS 8.1) is a Windows Network File System Remote Code Execution Vulnerability. If successful, it could allow a remote unauthenticated attacker to execute their code on an affected system with no user interaction. According to Microsoft, multiple exploit attempts may be required to do this, and it could go undetected unless there is an audit specifically monitoring for that activity. It is recommended for all users running NFS to patch immediately.

- CVE-2022-22038 (CVSS 8.1) is a Remote Procedure Call Runtime Remote Code Execution Vulnerability. According to Microsoft, this a high complexity attack as the threat actor would need to make "repeated exploitation attempts." If successful a remote unauthenticated threat actor could used to this vulnerability to exploit code on their target system. Successful exploitation of this vulnerability requires an attacker to invest time in repeated exploitation attempts through sending constant or intermittent data. Unless RPC activity is being actively blocked, these attempts may go undetected. It is recommended that users test and patch immediately.

To view the complete list of Microsoft vulnerabilities released in July 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

Google released an emergency patch this month for Chrome browser fixing four issues, including a zero-day flaw. Tracked as CVE-2022-2294 , this Heap buffer overflow in WebRTC in Google Chrome prior to 103.0.5060.114 allowed a remote threat actor to exploit heap corruption via a crafted HTML page. The memory corruption vulnerability in WebRTC(CVE-2022-2294) has been abused to achieve shellcode execution in Chrome's renderer process. It is worth noting this vulnerability was used in targeted attacks against Avast users in the Middle East, including journalists in Lebanon, to deliver spyware known as DevilsTongue. According to researchers, based on the malware and tactics used to conduct the attack, Avast attributes the use of the Chrome zero-day to Candiru, a secretive Israel-based company that sells spyware to governments. HC3 tracks global activity of this nature as it may have an impact on the United States. CISA encourages users and administrators to review the Chrome Release Note and apply the necessary update. Later in July, Google released Chrome version 103.0.5060.134 for Windows, Mac, and Linux which addresses vulnerabilities that a threat actor could exploit and take control of a target system. HC3 recommends administrators and users follow CISA's guidance to review the Chrome Release Note and apply the necessary updates immediately.
HC3 also 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. 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

Apple has released security updates including the latest version of iOS and iPadOS 15.6 to address 39 security vulnerabilities. Apple File System (APFS) tracked as CVE-2022-32832 is also included in this update. According to Apple, if exploited, this could provide an app the ability to execute code with kernel privileges allowing it to have deep access to a target device. Additional iOS 15.6 patches fix vulnerabilities in the kernel and WebKit browser engine, along with flaws in IOMobileFrameBuffer, Audio, iCloud Photo Library, ImageIO, Apple Neural Engine, and GPU Drivers. At this time, Apple is not aware of patched vulnerabilities being used in attacks, however the company states some of the vulnerabilities are serious, particularly those that affect the kernel at the heart of the operating system(OS). It is also worth noting that these vulnerabilities could be chained together in attacks. Apple also released security updates for watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, macOS Big Sur 11.6.8, and macOS Catalina 10.15.7 2022-005. CISA recommends administrators and users review the Apple security updates and apply necessary releases.

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 critical updates for Cisco Expressway Series, Cisco TelePresence Video Communication Server, Cisco Email Security Appliance, Cisco Secure Email and Web Manager, Cisco Small Business RV110W, RV130, RV130W, and RV215W routers, along with several other security updates for Cisco products. If successful, a threat actor could exploit some of these vulnerabilities to gain access and take control of a target system.

CISA encourages users and administrators to review the following Cisco advisories and apply the necessary updates:

- Cisco Expressway Series and Cisco TelePresence Video Communication Server Vulnerabilities cisco-sa-expressway-overwrite-3buqW8LH
- Cisco Smart Software Manager On-Prem Denial of Service Vulnerability cisco-sa-onprem-privesc-tP6uNZOS

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

Adobe released four advisories with updates to address 27 vulnerabilities affecting Adobe Acrobat, Character Animator, Photoshop, Reader, and RoboHelp. Of these 27 vulnerabilities, 18 are rated as 'Critical': ranging in severity from CVSS 6.5 to CVSS 7.8. The update for Acrobat and Reader addresses 22 different vulnerabilities with 'Critical' and 'Important' severity ratings. If a threat actor's attack is successful, the most severe of these could allow code execution if the threat actor is able to persuade a target to open a specially crafted PDF document. At this time there are no active attacks noted however Adobe classifies this as a Priority 2 deployment rating. The Photoshop update addresses one 'Critical' and one 'Important' rated flaw. The Critical bug is a use-after-free (UAF) that could lead to code execution. The patch for Character Animator addresses two 'Critical'-rated code execution flaws, one a heap overflow and the other an out-of-bounds (OOB) read. Finally, the patch for RoboHelp corrects a single Important-rated cross-site scripting (XSS) bug.

At the time of release, none of the vulnerabilities addressed by Adobe are listed as publicly known or under active attack. Adobe categorizes most of these updates as a deployment priority rating of three, with the Acrobat patch as the only exception with a 2 rating. 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 one security center advisory for their products this month. This advisory provides fixes or workarounds for vulnerabilities that are identified with Intel products. The following vulnerabilities were addressed:

- INTEL-SA-00702 (CVE-2022-28693, 4.7 CVSS score) & INTEL-SA-00707 (CVE-2022-29901, 4.7 CVSS score) - Intel Processors Return Stack Buffer Underflow Advisory – Some Intel Processors have a security vulnerability that could allow information disclosure. Non-transparent sharing of branch predictor targets between contexts in some Intel Processors could allow an authorized user to potentially enable information disclosure via local access. HC3 recommends users follow Intel's guidance which is for "affected Intel Processors use Indirect Branch Restricted Speculation (IBRS) instead of 'retpoline' to address this potential vulnerability." Additional information on "Retpoline: A Branch Target Mitigation" can be found by clicking here.

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

SAP

SAP has released 27 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 were no vulnerabilities with severity a rating of "Hot News" which the most severe rating, however there were 4 vulnerabilities with a "High" severity rating and 17 with a medium severity. A breakdown of advisories for vulnerabilities with a "High" severity rating are as follows:

- *Security Note#3221288 or CVE-2022-35228* (8.3 CVSS Score) - Information disclosure vulnerability in SAP BusinessObjects Business Intelligence Platform (Central management console).

- *Security Note#3212997 or CVE-2022-32249* (7.6 CVSS score) - Information Disclosure vulnerability in SAP Business One.

- *Security Note#3157613 or CVE-2022-28771* (7.5 CVSS score) - Missing Authentication check in SAP Business One (License service API).

- *Security Note#3191012 or CVE-2022-31593* (7.4 CVSS score) - Code Injection vulnerability in SAP Business One.

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 three security advisories this month, two with a 'Moderate' severity rating and one 'Low.' The moderate security advisories for July are as follows:

- VMSA-2022-0018 (CVE-2022-22982 , CVSS score 5.3) - VMware vCenter Server updates address a server-side request forgery vulnerability. This impacts products VMware vCenter Server (vCenter Server) and VMware Cloud Foundation (Cloud Foundation). If an attack is successful a threat actor with network access to 443 on the vCenter Server may exploit this issue by accessing a URL request outside of vCenter Server or accessing an internal service. It is recommended that users apply patches listed in the 'Fixed Version' column of the 'Response Matrix' by clicking here.

- VMSA-2022-0020 (CVE-2022-29901, CVE-2022-28693, CVE-2022-23816, CVE-2022-23825, CVSS score 5.6) - VMware ESXi addresses Return-Stack-Buffer-Underflow and Branch Type Confusion vulnerabilities. This impacts products VMware ESXi and VMware Cloud Foundation. VMware ESXi contains Return-Stack-Buffer-Underflow (CVE-2022-29901, CVE-2022-28693) and Branch Type Confusion (CVE-2022-23816, CVE-2022-23825) vulnerabilities caused by both the Intel and AMD processors it utilizes. A threat actor with unauthorized administrative access to a virtual machine has the ability take advantage of various side-channel CPU flaws that could leak information stored in physical memory about the hypervisor or other virtual machines that reside on the same ESXi host.

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

Android Security Bulletin – July 2022
https://source.android.com/security/bulletin/2022-07-01

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

Android and Google Service Mitigations
https://source.android.com/security/bulletin/2022-06-01#mitigations

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

Android Security Bulleting – July 2022
https://source.android.com/security/bulletin/2022-07-01

Apple Just Patched 39 iPhone Security Bugs
https://www.wired.com/story/apple-ios-google-chrome-security-updates-july-2022/

Apple Releases Security Updates for Multiple Products
https://www.cisa.gov/uscert/ncas/current-activity/2022/07/22/apple-releases-security-updates-multiple-products

Cisco Security Advisories
https://tools.cisco.com/security/center/publicationListing.x?product=Cisco&impact=critical,high&last_published=2022%20Jun&sort=-day_sir#~Vulnerabilities

Exploitation of Recent Chrome Zero-Day Linked to Israeli Spyware Company
https://www.securityweek.com/exploitation-recent-chrome-zero-day-linked-israeli-spyware-company

Google's July 2022 security patch is here for Pixel phones
https://www.androidpolice.com/july-2022-pixel-update/

Google Releases Security Update for Chrome
https://www.cisa.gov/uscert/ncas/current-activity/2022/07/05/google-releases-security-update-chrome

Google Releases Security Updates for Chrome
https://www.cisa.gov/uscert/ncas/current-activity/2022/07/21/google-releases-security-updates-chrome

Google's July 2022 security patch is here for Pixel phones
https://www.androidpolice.com/july-2022-pixel-update/

Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus
https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/

Intel Processors Return Stack Buffer Underflow Advisory
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00702.html

INTEL-SA-00702
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00702.html

INTEL-SA-00707
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00707.html

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

July 2022 Patch Tuesday forecast: A summertime lull?
https://www.helpnetsecurity.com/2022/07/08/july-2022-patch-tuesday-forecast/

July 2022 Patch Tuesday forecast: A summertime lull?
https://www.helpnetsecurity.com/2022/07/08/july-2022-patch-tuesday-forecast/

July 2022 Patch Tuesday | Microsoft Releases 84 Vulnerabilities with 4 Critical, plus 2 Microsoft Edge (Chromium-Based); Adobe Releases 4 Advisories, 27 Vulnerabilities with 18 Critical.
https://blog.qualys.com/vulnerabilities-threat-research/2022/07/12/july-2022-patch-tuesday

July 2022 Patch Tuesday forecast: A summertime lull?
https://www.helpnetsecurity.com/2022/07/08/july-2022-patch-tuesday-forecast/

Microsoft Security Update Guide
https://isc.sans.edu/diary/Microsoft+July+2022+Patch+Tuesday/28838

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

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

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

Microsoft Patch Tuesday, July 2022 Edition
https://krebsonsecurity.com/2022/07/microsoft-patch-tuesday-july-2022-edition/

Microsoft July 2022 Patch Tuesday fixes exploited zero-day, 84 flaws
https://www.bleepingcomputer.com/news/microsoft/microsoft-july-2022-patch-tuesday-fixes-exploited-zero-day-84-flaws/

Return Stack Buffer Underflow / Return Stack Buffer Underflow / CVE-2022-29901, CVE-2022-28693 / INTEL-SA-00702
https://www.intel.com/content/www/us/en/developer/articles/technical/software-security-guidance/advisory-guidance/return-stack-buffer-underflow.html

Retpoline: A Branch Target Injection Mitigation

https://www.intel.com/content/www/us/en/developer/articles/technical/software-security-guidance/technical-documentation/retpoline-branch-target-injection-mitigation.html

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

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

The July 2022 Security Update Review
https://www.zerodayinitiative.com/blog/2022/7/12/the-july-2022-security-update-review

The Return of Candiru: Zero-days in the Middle East
https://decoded.avast.io/janvojtesek/the-return-of-candiru-zero-days-in-the-middle-east/

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