HC3: Monthly Cybersecurity Vulnerability Bulletin

May 6, 2022 TLP: White Report: 202205061200

April Vulnerabilities of Interest to the Health Sector

Executive Summary

In April 2022, vulnerabilities in common information systems relevant 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, Adobe, Android, Google, Apple, CISCO, Mozilla, Oracle, SAP, SonicWall, and VMWare. HC3 recommends patching all vulnerabilities with special consideration to each vulnerability criticality category against the risk management posture of the organization.

Importance to HPH Sector

DEPARTMENT OF HOMELAND SECURITY/CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

In April, the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) added 22 vulnerabilities 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

For the month of April, Microsoft released patches for a total of 145 vulnerabilities. 128 new patches were for CVEs in Microsoft Windows and Windows Components, Microsoft Defender and Defender for Endpoint, Microsoft Dynamics, Microsoft Edge (Chromium-based), Exchange Server, Office and Office Components, SharePoint Server, Windows Hyper-V, DNS Server, Skype for Business, .NET and Visual Studio, Windows App Store, and Windows Print Spooler Components. In addition to this, 17 flaws were found in Chromium Open-Source Software (OSS) by Microsoft Edge (Chromium-based). The severity ratings for the 128 CVEs released on Patch Tuesday are as follows: 10 Critical, 115 Important, and three are moderate. This is patch Tuesday has the largest number of vulnerabilities since September 2020. Some notable vulnerabilities are as follows:

- Windows Hyper V had the following critical vulnerabilities patched: CVE-2022-23257, CVE-2022-24537 and CVE-2022-22008; these flaws could lead to remote code execution. If a threat actor is able to open a specially crafted file, followed by and application on a Hyper-V guest, then that could cause the Hyper-V host operating system to execute arbitrary code.
- Windows Network File system also had two critical remote code execution vulnerabilities: CVE-2022-24491 and CVE-2022-24497; these can only be exploited on Windows Server systems that have the NFS role enabled.

HC3: Monthly Cybersecurity Vulnerability Bulletin

May 6, 2022 TLP: White Report: 202205061200

A "wormable" vulnerability is one that can launch an attack and spread without human interaction. These types of CVE's can have a significant impact if the number of vulnerable machines is high enough. Web application firewalls (WAFs) would help to mitigate the risk in situations like this. Here are some noteworthy "Critical-rated" flaws from this month that could be "wormable":

- CVE-2022-26809 (CVSS 9.8) - RPC Runtime Library Remote Code Execution Vulnerability
- CVE-2022-24491/24497 (CVSS 9.8) – Windows Network File System Remote Code Execution Vulnerability
- CVE-2022-26815 (CVSS 7.2) - Windows DNS Server Remote Code Execution Vulnerability
- CVE-2022-26904 (CVSS 7.0) – Windows User Profile Service Elevation of Privilege Vulnerability

CVE-2022-24491 is the publicly known zero-day is a privilege elevation bug. In addition to this, CVE-2022-26904 is the actively exploited zero-day vulnerability fixed this month that a security researcher discovered that Microsoft addressed twice before after new patch bypasses were found. To view the list of Microsoft vulnerabilities released by in April and their rating click here. HC3 recommends patching and testing immediately as all vulnerabilities can adversely impact the Health sector.

ADOBE

In April, Adobe released four patched for to fix 70 vulnerabilities in Acrobat, Reader, After Effects, Photoshop, and Adobe Commerce. There was a total of 62 CVEs for the updates for Acrobat and Reader. Critical-Rated Use-After-Free (UAF) and Out-of-Bounds (OOB) Write claws were among the more severe CVE's addressed. If a threat actor is able to convince a user to open a specific PDF document, then the attacker could successfully execute code on a target system. You can find additional information on those updates, by clicking here. In addition to this, there were 13 vulnerabilities addressed for Photoshop. All of them Critical-rated code execution flaws. If a threat actor can get a user to open a specific file, then the attacker could gain code execution. Additional information for this update is available by clicking here. Two Critical-rated vulnerabilities listed as stack based-buffer overflows that could allow for code execution were also addressed in the updates for Adobe After Effects(Windows and Mac OS). The Adobe Commerce and Magento Open-Source patch fixed a single vulnerability with a critical rating and a CVSS 9.1. If a threat actor exploited this vulnerability, it could lead to arbitrary code execution. You can view additional information on this product by clicking here. At this time, none of the vulnerabilities fixed by Adobe are listed as publicly known or under active attack. 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.

ANDROID / GOOGLE

For the month of April, the Android updates released by Google include patches for 44 vulnerabilities, several that with a critical severity rating. The first of two updates for this month, was on April 1st and it addressed 14 security flaws. Google's advisory stated, "The most severe of these issues is a high security vulnerability in the Framework component that could lead to local escalation of privilege with no additional execution privileges needed." Seven "high severity" rating vulnerabilities all leading to elevation of privilege, were resolved in the Framework component this month. Patches for two issues in Media framework, three in System, two Google Play system updates resolving two vulnerabilities in MediaProvider

and Media Codecs were also included in the April 1st security update. The second part of April's security update was on April 5th and included patches for about 30 vulnerabilities in System, Kernel components, MediaTek components, Qualcomm components, and Qualcomm closed-source components. Nine of these vulnerabilities have a "critical" severity rating, all impacting affecting Qualcomm components. The remaining 21 have a "high severity" rating. In addition to this, Google released patches for vulnerabilities for Pixel devices addressing Kernel components, Pixel, and Qualcomm components as well. 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. 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 April's parch Tuesday Apply released fixes to address two zero-day vulnerabilities (CVE-2022-22675 and CVE-2022-22674)impacting Macs, iPads, and iPhones. One zero day, CVE-2022-22675 , is connected to an out of bounds write issue that impacts the AppleAVD media decoder. If a threat actor successfully exploits this vulnerability the attacker would be able to take full control of the device and execute arbitrary code with kernel privileges. Apple was able to address this vulnerability with improved bounds checking. The second zero day CVE-2022-22674 is an out-of-bounds read issue impacting the Intel Graphics driver that could lead to the disclosure of kernel memory. Apple addressed this issue with improved input validation. The update for Macs is included in macOS Monterey 12.3.1; iPhones and iPads have updates in iOS 15.4.1 and iPadOS 15.4.1. The fix is specifically for iPhone 6s models and later, all iPad Pro models, iPad Air 2 and later, iPad 5th generation and later, iPad mini 4 and later, and iPod touch (7th generation). For a complete list of the latest Apple security and software updates click here. HC3 recommends installing updates and applying patches immediately to prevent potential attacks. According to Apple, after a software update is installed for iOS, iPadOS, tvOS, and watchOS, it cannot be downgraded to the previous version.

CISCO

For the month of April, security updates to address vulnerabilities in several Cisco products were released. If successful, a threat actor could exploit these vulnerabilities and take control of the targeted system. HC3 recommends users and administrators follow CISA's guidance, which is to review the following Cisco advisories and apply the necessary updates:

- Cisco Virtualized Infrastructure Manager Privilege Escalation Vulnerability cisco-sa-vim-privesc-T2tsFUf
- Cisco Umbrella Virtual Appliance Static SSH Host Key Vulnerability cisco-sa-uva-static-key-6RQTRs4c
- Cisco TelePresence Collaboration Endpoint and RoomOS Software H.323 Denial of Service Vulnerability cisco-sa-ce-roomos-dos-c65x2Qf2

For a complete list of updates for vulnerabilities including those with a lower severity rating visit the Cisco Security Advisories page by clicking here.

HC3: Monthly Cybersecurity Vulnerability Bulletin

May 6, 2022 TLP: White Report: 202205061200

MOZILLA

This month, Mozilla released updates for to address three vulnerabilities with "high" severity ratings. MFSA 2022-15 addresses security vulnerabilities fixed in Thunderbird 91.8; MFSA 2022-14 addresses security vulnerabilities fixed in Firefox ESR 91.8; MFSA 2022-13 addresses security vulnerabilities fixed in Firefox 99. HC3 recommends that all users, review Mozilla security advisories and apply the necessary patches immediately.

ORACLE

For the month of April, Oracle released 520 new security updates for vulnerabilities in Oracle code and in third-party components included in Oracle products. To view the complete list of critical patch updates, security alerts, and bulletins click here. HC3 recommends patching and updating immediately. For a complete list of vulnerabilities addressed, affected products, and workarounds for the month of April click here.

SAP

For April's Patch Tuesday, SAP released more than 30 new and updated security notes including notes pertaining to the Spring4Shell vulnerability. The Spring4Shell vulnerability (CVE-2022-22965) impacts Spring, a Java application development framework. If a threat actor is successful, this could lead to remote code execution. It is worth mentioning, that some researchers have reported observing attempts to exploit this vulnerability in the wild. In addition to this, SAP also published three "Hot News" rated security notes pertaining to Spring4Shell. Other noteworthy "Hot News" notes released this month included an update Chromium-based browser in Business Client. 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.

SonicWall

This month, SonicWall released patches to address three zero-day vulnerabilities to its hosted and on-premises email security products. CVE-2021-20021, CVE-2021-20022, and CVE-2021-20023 are the three vulnerabilities affecting SonicWall Email Security products. Additional information on each CVE can be viewed by clicking here. If successful, a remote threat actor can exploit these vulnerabilities and take control of an affected system. Sonic Wall also stated that, "In at least one known case, these vulnerabilities have been observed to be exploited 'in the wild.'" A complete list of Sonic Wall's affected products, updates, and workarounds can be viewed on SonicWall's Security advisory clicking here. HC3 recommends users apply all patches and updates immediately and follow SonicWall PSIRT's guidance.

VMWARE

This month VMWare released updates for eight vulnerabilities in its products, some of which could be exploited to launch remote code execution attacks. Five of these vulnerabilities have a severity rating of Critical, two as Important, and one as Moderate. The most notable flaws this month are as follows:

- CVE-2022-22954 (9.8 CVSS score) - Server-side template injection remote code execution vulnerability affecting VMware Workspace ONE Access and Identity Manager

- CVE-2022-22955 & CVE-2022-22956 (9.8 CVSS score) - OAuth2 ACS authentication bypass vulnerabilities in VMware Workspace ONE Access

- CVE-2022-22957 & CVE-2022-22958 (9.1 CVSS score) - JDBC injection remote code execution vulnerabilities in VMware Workspace ONE Access, Identity Manager, and vRealize Automation

- CVE-2022-22959 (8.8 CVSS score) - Cross-site request forgery (CSRF) vulnerability in VMware Workspace ONE Access, Identity Manager, and vRealize Automation

- CVE-2022-22960 (7.8 CVSS score) - Local privilege escalation vulnerability in VMware Workspace ONE Access, Identity Manager and vRealize Automation

- CVE-2022-22961 (5.3 CVSS score) - Information disclosure vulnerability impacting VMware Workspace ONE Access, Identity Manager and vRealize Automation

HC3 recommends VMWare users check for frequent updates, keep software updated, and to apply patches immediately. For a complete list of this month's VMWare Security advisories click here.

Recently Published Information

44 Vulnerabilities Patched in Android With April 2022 Security Updates
https://www.securityweek.com/44-vulnerabilities-patched-android-april-2022-security-updates

Apple releases fixes for two zero-days affecting Macs, iPhones and iPads
https://therecord.media/apple-releases-fixes-for-two-zero-days-affecting-macs-iphones-and-ipads/

Apple Releases Security Updates
https://www.cisa.gov/uscert/ncas/current-activity/2022/04/01/apple-releases-security-updates-0

April 2022 Patch Tuesday forecast: Spring is in the air (and vulnerable)
https://www.helpnetsecurity.com/2022/04/08/april-2022-patch-tuesday-forecast/

Cisco Releases Security Updates for Multiple Products
https://www.cisa.gov/uscert/ncas/current-activity/2022/04/14/cisco-releases-security-updates-multiple-products

Cisco Releases Security Updates for Multiple Products
https://www.cisa.gov/uscert/ncas/current-activity/2022/04/21/cisco-releases-security-updates-multiple-products-0

Google Releases Security Updates for Chrome
https://www.cisa.gov/uscert/ncas/current-activity/2022/04/15/google-releases-security-updates-chrome

Microsoft April 2022 Patch Tuesday fixes 119 flaws, 2 zero-days
https://www.bleepingcomputer.com/news/microsoft/microsoft-april-2022-patch-tuesday-fixes-119-flaws-

2-zero-days/

Microsoft's April 2022 Patch Tuesday tackles two zero-day vulnerabilities
https://www.zdnet.com/article/microsoft-april-2022-patch-tuesday-two-zero-day-vulnerabilities-tackled/

Microsoft Patch Tuesday, April 2022 Edition
https://krebsonsecurity.com/2022/04/microsoft-patch-tuesday-april-2022-edition/

Microsoft Patch Tuesday includes most vulnerabilities since Sept. 2020
https://blog.talosintelligence.com/2022/04/microsoft-patch-tuesday-includes-most.html

Oracle Critical Patch Update Advisory - April 2022
https://www.oracle.com/security-alerts/cpuapr2022.html

SAP Releases Patches for Spring4Shell Vulnerability
https://www.securityweek.com/sap-releases-patches-spring4shell-vulnerability

SonicWall Releases Patches for Email Security Products
https://www.cisa.gov/uscert/ncas/current-activity/2021/04/21/sonicwall-releases-patches-email-security-products

VMware Releases Critical Patches for New Vulnerabilities Affecting Multiple Products
https://thehackernews.com/2022/04/vmware-releases-critical-patches-for.html

Contact Information

If you have any additional questions, please contact us at HC3@hhs.gov.

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback