HC3: Monthly Cybersecurity Vulnerability Bulletin

March 18, 2022 TLP: White Report: 202203181300

February Vulnerabilities of Interest to the Health Sector

Executive Summary

In February 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, Citrix, Intel, Mozilla, SAP, and VMWare. HC3 recommends patching all vulnerabilities with special consideration to each vulnerability criticality category against the risk management posture of the organization. As always, accountability, proper inventory management and device hygiene along with and asset tracking are imperative to an effective patch management program.

Importance to HPH Sector

DEPARTMENT OF HOMELAND SECURITY/CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

The Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) is constantly adding new 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 February, Microsoft released 48 security fixes for software, including a patch for a zero-day vulnerability. There were no critical-severity flaws on the list for this month. Microsoft Outlook and Office, Azure Data Explorer, Windows Kernel, Hyper-V, and Microsoft SharePoint are some of the product's impacted by this month's update.

CVE-2022-21989 is the single Zero-day vulnerabilities released in Microsoft's updates for this month. It has a CVSS severity score of 7.8 , a high attack complexity, and this publicly known flaw can be exploited to escalate privileges via the kernel. According to Microsoft, to trigger this exploit a threat actor would have to take additional actions prior to exploitation to prepare the target environment. Additional vulnerabilities of interest in this update are:

- CVE-2022-21989 is a Windows Kernel elevation-of-privilege vulnerability. According to the Microsoft advisory, successful exploitation of this vulnerability requires a threat actor to take additional actions prior to exploitation to prepare the target environment. A successful attack could be performed from a low privilege AppContainer and the threat actor could elevate their privileges and execute code or access resources at a higher integrity level than that of the AppContainer execution environment.

- CVE-2022-21996 is a Win32k elevation of privilege vulnerability listed as more likely to be exploited. The attack may be initiated remotely and only requires simple authentication for exploitation.
- CVE-2022-22005 is a Microsoft SharePoint Server Remote Code Execution vulnerability. The attacker must be authenticated and possess the permissions for page creation to be able to exploit this vulnerability. This permission however is often present for an authenticated user.
- CVE-2022-21984 is a Windows DNS Server Remote Code Execution vulnerability. The server is only affected if dynamic updates are enabled, however this is a relatively common configuration. A threat actor might take control of their target's DNS and execute code with elevated privileges if this is set up in the target's environment.

With the amount of stolen login credentials available, it is recommended that organizations pay attention to vulnerabilities that require authentication, particularly when it comes to public-facing servers. Microsoft has a *Security Update Guide* notification system that accepts standard email addresses during signup rather than only Live IDs. HC3 recommends patching and testing immediately as all vulnerabilities can adversely impact the healthcare industry. For the entire list of vulnerabilities released by Microsoft this month and their rating click here.

ADOBE

In February Adobe released security updates to fix 17 CVEs affecting Premiere Rush, Illustrator, Photoshop, AfterEffects, and Creative Cloud Desktop Application. Of these 17 vulnerabilities, five (5) are treated as Critical. The Critical vulnerabilities of note are as follows:

- CVE-2022-23203 A buffer overflow vulnerability that could lead to arbitrary code execution in Photoshop 2021 and Photoshop 2022 for Windows and macOS.
- CVE-2022-23186 An out-of-bounds write vulnerability that could lead to arbitrary code execution in Illustrator 2021 and Illustrator 2022 for Windows and macOS.
- CVE-2022-23188 A buffer overflow vulnerability that could lead to arbitrary code execution in Illustrator 2021 and Illustrator 2022 for Windows and macOS.
- CVE-2022-23200 An out-of-bounds write vulnerability that could lead to arbitrary code execution in Adobe After Effects 18.4.3, 22.1.1 and earlier versions for Windows and macOS.
- CVE-2022-23202 Uncontrolled search path element vulnerability that could lead to arbitrary code execution in the Creative Cloud Desktop Application installer 2.7.0.13 and earlier versions on Windows.

Successful exploitation of these vulnerabilities could lead to application denial-of-service (DoS), arbitrary code execution, privilege escalation, and memory leaks. HC3 recommends applying the appropriate security updates or patches that can be found on Adobe's Product Security Incident Response Team (PSIRT) by clicking here because an attacker could exploit some of these vulnerabilities to control of a compromised system.

ANDROID / GOOGLE

For the month of February, Google announced that Android security updates included patches for a total of 36 vulnerabilities. The first part of the update, released February 1st, provided fixes for 15 security holes in three components, including Framework, Media framework, and System. Google identified CVE-2021-39675 as the most severe of these issues. It is a critical vulnerability in the System component that could

be exploited to elevate privileges. The remaining 14 issues are rated high severity, five of them impact Framework (four elevation of privilege and one information disclosure bug), four were fixed in the Media framework (two elevation of privilege and two information disclosure flaws), and five were identified in the System component (four elevation of privilege and one DoS vulnerability).

On February 5th the second part of security updates were released and addressed 21 additional vulnerabilities in System (1), Amlogic components (1), MediaTek components (5), Unisoc components (3), Qualcomm components (5), and Qualcomm closed-source components (6). In an Android advisory, Google announced the release of patches for four security holes affecting its Pixel devices. These were addressed in Pixel (two high-severity information disclosure bugs) and Qualcomm components (two moderate-severity errors). According Google, Android and Pixel devices running a security patch level of February 5, 2022 or later are protected against all of these vulnerabilities as well as previously patched issues. 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 the month of February, Apple has released security updates to fix a zero-day vulnerability (CVE-2022-22620) exploited in the wild by attackers to hack iPhones, iPads, and Macs.

The zero-day patched is CVE-2022-22620 [1, 2] and it is a Webkit "Use After Free" issue that can lead to OS crashes and code execution on devices that are compromised. Apple addressed this vulnerability with improved management in iOS 15.3.1, iPadOS 15.3.1, and MacOS Monterey 12.2.1. This vulnerability affects both older and newer models and it includes the following:

- All models of iPad Pro
- iPhone 6s and later, iPad Air 2 and later
- iPad 5th generation and later, iPad mini 4 and later
- 7th generation of iPod touch
- Macs running macOS Monterey

HC3 recommends installing updates and applying patches immediately to prevent potential attacks. For a complete list of the latest Apple security and software updates click here. 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 February Cisco released 9 security advisories, 1 classified as Critical and 8 as High. The critical advisory for Cisco Small Business RV Series Routers Vulnerabilities involves Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an attacker to do any of the following:

- Execute arbitrary code
- Elevate privileges
- Execute arbitrary commands
- Bypass authentication and authorization protections
- Fetch and run unsigned software
- Cause denial of service (DoS)

Cisco has released software updates that address these vulnerabilities. Currently, there are no workarounds that address these vulnerabilities. Vulnerable Products are as follows: CVE-2022-20700, CVE-2022-20702, CVE-2022-20703, CVE-2022-20704, CVE-2022-20705 and CVE-2022-20706 affect the following Cisco products: RV160 VPN Routers, RV160W Wireless-AC VPN Routers, RV260 VPN Routers, RV260P VPN Routers with PoE, RV260W Wireless-AC VPN Routers, RV340 Dual WAN Gigabit VPN Routers, RV340W Dual WAN Gigabit Wireless-AC VPN Routers, RV345 Dual WAN Gigabit VPN Routers, RV345P Dual WAN Gigabit POE VPN Routers.
In additional to this, CVE-2022-20699, CVE-2022-20701, CVE-2022-20707, CVE-2022-20708, CVE-2022-20709, CVE-2022-20710, CVE-2022-20711, CVE-2022-20712 and CVE-2022-20749 affect only the following Cisco products: RV340 Dual WAN Gigabit VPN Routers, RV340W Dual WAN Gigabit Wireless-AC VPN Routers, RV345 Dual WAN Gigabit VPN Routers, and RV345P Dual WAN Gigabit POE VPN Routers.
HC3 Recommends keeping software current and applying patches as soon as they are available. In addition to this, the Cisco's vulnerable products section provides Cisco bug IDs for each product. All vulnerabilities are accessible through the Cisco Bug Search Tool and will contain specific information, fixed software releases, and workarounds (if available).

CITRIX

For the month of February, Citrix released security updates to address vulnerabilities in Hypervisor. If successful, a threat actor can exploit these vulnerabilities to cause a denial-of-service attack. Vulnerabilities that can cause security issues that affect Hypervisor are CVE-2022-23034, CVE-2022-23035 , and CVE-2021-0145. Citrix has released hotfixes to address these issues.
HC3 recommends users follow Citrix's guidance "that affected customers install these hotfixes" along with any necessary updates and patches immediately. The hotfixes can be downloaded from the following locations: Citrix Hypervisor 8.2 CU1 LTSR: CTX338451 , Citrix Hypervisor 8.2: CTX338452, and Citrix XenServer 7.1 CU2 LTSR: CTX338453. The latest version of Citrix Workspace app for Linux is available and can be accessed by clicking here.

INTEL

Intel released several security advisories for the month of February. The Intel Quartus Advisory (INTEL-SA-00632) is a security advisory of note this month with a High severity rating. A few vulnerabilities related to INTEL-SA-00632 with a classification of High in severity are as follows:

- CVE-2022-21203 involves improper permissions in the SafeNet Sentinel driver for Intel(R) Quartus(R) Prime Standard Edition before version 21.1 may allow an authenticated user to potentially enable escalation of privilege via local access. The vulnerability has a High CVSS base score of 8.8.

- CVE-2021-44454 involves improper input validation in a third-party component for Intel(R) Quartus(R) Prime Pro Edition before version 21.3 may allow an authenticated user to potentially enable escalation of privilege via local access. The vulnerability has a High CVSS base score of 7.3.

For a complete list of Intel's security advisories and their vulnerabilities for February click here. With the INTEL-SA-00632 security advisory, the potential security vulnerabilities in Intel Quartus Prime Pro and Standard Editions could allow escalation of privilege, denial of service, or information disclosure. HC3 recommends following Intel's guidance which is updating Intel Quartus Prime Pro to version 21.3 or later and Intel Quartus Prime Standard Edition to version 21.1 or later. Intel has updates available for download and you can access this by clicking here. A complete list of security advisories can be accessed on Intel's Product Security Center Advisories page.

MOZILLA

This month Mozilla fixed a dozen security vulnerabilities in its Firefox browser. The two most important to note are both regarding permissions issues:

- CVE-2022-22753 - A Time-of-Check Time-of-Use bug existed in the Maintenance (Updater) Service that could be abused to grant users write access to an arbitrary directory. This could have been used to escalate to SYSTEM access. This bug only affects Firefox on Windows. Other operating systems are unaffected.
- CVE-2022-22754 - If a user installs an extension of a particular type, the extension could have auto-updated itself and in the process of doing so, bypass the prompt which grants the new version its new requested permissions.

In addition to this, there were two vulnerabilities (CVE-2022-22764 , CVE-2022-0511)classified as High found by Mozilla developers this month. CVE-2022-22764 and CVE-2022-0511 are both memory safety vulnerabilities that with enough effort can be exploited to run arbitrary code. HC3 recommends all users, review Mozilla security advisories and apply necessary updates and patches immediately.

SAP

For February's Patch Tuesday, SAP published 9 security notes classified as Hot News (CVSS 9.1 – 10) and 3 High Priority (CVSS 7.1-8.7). Some vulnerabilities of note are as follows:

- CVE-2022-22536 (Security Note: 3123396, CVSS: 10) – SAP NetWeaver Application Server ABAP, SAP NetWeaver Application Server Java, ABAP Platform, SAP Content Server 7.53 and SAP Web Dispatcher are all vulnerable for request smuggling and request concatenation. If successful, an unauthenticated threat actor could prepend a victim's request with arbitrary data. This would allow the threat actor to execute functions impersonating the victim or poison intermediary Web caches and could result in the compromise of Confidentiality, Integrity and Availability of the targeted system.

- CVE-2021-44228 (Security Note: 3123396, CVSS: 10) – Remote Code Execution vulnerability associated with Apache Log4j 2 component used in SAP Commerce. Apache Log4j2 2.0-beta9 through 2.15.0 (security releases 2.12.2, 2.12.3, and 2.3.1 are excluded) JNDI features used in configuration, log messages, and parameters do not protect against attacker-controlled LDAP and other JNDI related endpoints. A threat actor who can control log messages or log message

parameters has the ability to execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. This vulnerability does not affect log4net, log4cxx, or other Apache Logging Services projects and is specific to log4j-core.

For a complete list of SAP's patch day vulnerabilities click here. HC3 recommends patching immediately and following SAP's guidance for additional support. To fix vulnerabilities discovered in SAP products, SAP recommends customer visit the Support Portal and apply patches protect their SAP landscape.

VMWARE

In February's Patch Tuesday VMWare released 11 security advisories, 4 were classified as Critical and 4 as Important. Some critical security advisories are as follows:

- VMSA-2022-0004 has a maximum CVSSv3 base score of 8.4. VMware ESXi, Workstation, and Fusion contain a use-after-free vulnerability in the XHCI USB controller. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. With privileges within the VMX process only, the threat actor could be able to access the settings service running as a high privileged user. Click here to view the 'fixed version' column of the "response matrix' for following: CVE-2021-22040, CVE-2021-22041, CVE-2021-22042, CVE-2021-22043, CVE-2021-22050.
- VMSA-2021-0028.13 has a maximum CVSSv3 base score of 10. Multiple products impacted by remote code execution vulnerabilities via Apache Log4j (CVE-2021-44228, CVE-2021-45046). A malicious actor with network access to an impacted VMware product may exploit these issues to gain full control of the target system. Workarounds and fixes for CVE-2021-44228, CVE-2021-45046 can be found in the 'Fixed Version' column of the 'Response Matrix' by clicking here.

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

Recently Published Information

Android's February 2022 Security Updates Patch 36 Vulnerabilities
https://www.securityweek.com/androids-february-2022-security-update-patches-36-vulnerabilities

Apple patches new zero-day exploited to hack iPhones, iPads, Macs
https://www.bleepingcomputer.com/news/security/apple-patches-new-zero-day-exploited-to-hack-iphones-ipads-macs/

Chrome Zero-Day Under Active Attack: Patch ASAP
https://threatpost.com/google-chrome-zero-day-under-attack/178428/

Cisco Releases Security Updates for Email Security Appliance
https://www.cisa.gov/uscert/ncas/current-activity/2022/02/17/cisco-releases-security-updates-email-security-appliance

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

Citrix Releases Security Updates for Hypervisor
https://www.cisa.gov/uscert/ncas/current-activity/2022/02/08/citrix-releases-security-updates-hypervisor

Microsoft February 2022 Patch Tuesday fixes 48 flaws, 1 zero-day
https://www.bleepingcomputer.com/news/microsoft/microsoft-february-2022-patch-tuesday-fixes-48-flaws-1-zero-day/

Microsoft February 2022 Patch Tuesday: 48 bugs squashed, one zero-day resolved
https://www.zdnet.com/article/microsoft-february-2021-patch-tuesday-48-bugs-squashed-one-zero-day-resolved/

Microsoft Patch Tuesday, February 2022 Edition
https://krebsonsecurity.com/2022/02/microsoft-patch-tuesday-february-2022-edition/

SAP Security Patch Day – February 2022
https://wiki.scn.sap.com/wiki/display/PSR/SAP+Security+Patch+Day+-+February+2022

Update now! Firefox and Adobe updates are more critical than Microsoft's
https://blog.malwarebytes.com/exploits-and-vulnerabilities/2022/02/update-now-firefox-and-adobe-updates-are-more-critical-than-microsofts/

VMWare Security Advisories
https://www.vmware.com/security/advisories.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