HC3: Monthly Cybersecurity Vulnerability Bulletin
March 13, 2023 TLP:CLEAR Report: 202303131700

February Vulnerabilities of Interest to the Health Sector

In February 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 this month are from Microsoft, Google/Android, Apple, Mozilla, SAP, Citrix, Intel, Cisco, VMWare, Fortinet, 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 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 14 vulnerabilities in February 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

Microsoft released security updates to fix three actively exploited zero-day vulnerabilities and a total of 77 flaws. Nine vulnerabilities have been classified as 'Critical,' which is one of the most severe types of vulnerabilities, as they allow remote code execution, bypass security features, or elevate privileges. The number of bugs in each vulnerability category is listed as follows:

- 12 Elevation of Privilege Vulnerabilities
- 2 Security Feature Bypass Vulnerabilities
- 38 Remote Code Execution Vulnerabilities
- 8 Information Disclosure Vulnerabilities
- 10 Denial of Service Vulnerabilities
- 8 Spoofing Vulnerabilities

The count above does not include three Microsoft Edge vulnerabilities fixed in the month. February's Patch Tuesday also addressed the following actively exploited zero-day vulnerabilities used in attacks. Additional information on these vulnerabilities are as follows:

- CVE-2023-23376 - *Windows Common Log File System Driver Elevation of Privilege Vulnerability* – This vulnerability allows a threat actor who successfully exploits this zero-day vulnerability the ability to gain SYSTEM privileges.

- CVE-2023-21715 - *Microsoft Publisher Security Features Bypass Vulnerability* – This vulnerability is in Microsoft Publisher and allows a specially crafted document to bypass Office macro policies that block untrusted or malicious files. If a threat actor is successful, exploiting this flaw would effectively allow macros in a malicious Publisher document to run without first warning the user. According to Microsoft, "The attack itself is carried out locally by a user with authentication to the targeted system." Additionally, an attacker that receives authentication can exploit this vulnerability by using social engineering to convince a victim "to download and open a specially crafted file from a website which could lead to a local attack on the victim computer."
- CVE-2023-21823 - *Windows Graphics Component Remote Code Execution Vulnerability* – According to Microsoft this remote code execution vulnerability allows attackers to execute commands with SYSTEM privileges. It is important to note, that this security update will be pushed out to users through the Microsoft Store instead of Windows Update. Customers who disable automatic updates in the Microsoft Store should manually look for this update.

For a complete list of Microsoft vulnerabilities released in February 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 released patches for 40 vulnerabilities that are addressed in Android's security bulletin affecting devices running Android's operating system. Every month, security updates are released in two parts. The first part of the update arrived on devices as a 2023-02-01 security patch level and fixed 17 'High severity' vulnerabilities affecting components such as Media Framework, Framework, and System. While many of the vulnerabilities fixed in the first update could lead to escalation of privilege, information disclosure and denial-of-service (DoS) flaws were also addressed. According to Google, a "High security vulnerability in the Framework component that could lead to local escalation of privilege with no additional execution privileges needed" is the most severe of these issues. The second part of the update arrived on devices as the *2023-02-05 security patch level* and fixed 23 security defects in MediaTek, Unisoc, Kernel, Qualcomm, and Qualcomm closed-source components. Google also addressed three vulnerabilities specific to Pixel devices. All Pixels running a patch level of 2023-02-05 will be patched against these three vulnerabilities and all issues will be resolved with Android's February 2023 security update. Additionally, Google released one patch as a part of February's Android Automotive OS (AAOS) update along with source code patches to the Android Open-Source Project (AOSP) repository.

HC3 recommends that 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 security vulnerabilities affecting Android devices can be viewed by clicking here.

Apple

Apple released security updates to address vulnerabilities in multiple products. If successful, a remote threat actor can exploit these vulnerabilities and take control of a compromised device or system. HC3 recommends all users and administrators follow CISA's guidance which "encourages users and administrators to review Apple's security updates page and apply the necessary updates for the following:

- Safari 16.3.1
- iOS 16.3.1 and iPadOS 16.3.1
- macOS 13.2.1

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

Mozilla

Mozilla released several security updates addressing vulnerabilities in vulnerabilities in Firefox 110, Firefox ESR 102.8, and Thunderbird 102.8. If successful, a threat actor could exploit these vulnerabilities and take control of a compromised device or system. HC3 encourages all users to follows CISA's guidance which is "to review Mozilla's security advisories for Firefox 110,Firefox ESR 102.8 , and Thunderbird 102.8" for additional information and apply necessary patches or updates immediately.

SAP

SAP released 21 new security notes and five updates to previously issued security notes, to address vulnerabilities affecting multiple products. If successful with launching an attack, a threat actor could exploit these vulnerabilities and take control of a compromised device or system. For February there was one vulnerability with a severity rating of "Hot News" which is the most severe rating. There were also five flaws classified as "High" and 15 as "Medium" in severity. A breakdown of some security notes for vulnerabilities with "Hot News" and "High" severity ratings are as follows:

- Security Note# 2622660 has a 10.0 CVSS score and "Hot News" severity rating. This is an update to a security note released in April 2018 on Patch Day; security updates for the browser control Google Chromium delivered with SAP Business Client. Product(s) impacted: SAP Business Client, Versions – 6.5, 7.0,7.70.
- Security Note#3285757 (CVE-2023-24523) has a 8.8 CVSS score and "High" severity rating. This is a privilege escalation vulnerability in SAP start service. Product(s) impacted: SAP Host Agent Service, Versions -7.21, 7.22.
- Security Note# 3268172 (CVE-2022-41264) has a 8.8 CVSS score and "High" severity rating. This is an update to a security note released on Patch Tuesday in December 2022 for a code injection vulnerability in SAP BASIS. Product(s) impacted: APBASIS, Versions –731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, 791.

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.

Intel

Intel issued 31 security center advisories for their products, and the patches addressed five SGX-related vulnerabilities. Two of SGX vulnerabilities include a potential privilege escalation that could result in information disclosure and enable secure processing of sensitive data inside encrypted memory areas or enclaves. These advisories provide fixes and workarounds for vulnerabilities that are identified with Intel products. The following is additional on information on some notable vulnerabilities addressed this month:

- INTEL-SA-00717 2023.1 IPU - BIOS Advisory - Potential security vulnerabilities in the BIOS firmware and Intel Trusted Execution Technology (TXT) Secure Initialization (SINIT) Authenticated Code Modules (ACM) for some Intel Processors may allow escalation of privilege. Intel is releasing BIOS updates to mitigate these potential vulnerabilities. High severity vulnerabilities related to this advisory are as follows: CVE-2022-26343 (CVSS base score 8.2), CVE-2022-30539 (CVSS base score 7.5), CVE-2022-32231 (CVSS base score 7.5), CVE-2022-26837 (CVSS base score 7.5), CVE-2022-30704 (CVSS base score 7.2)
- INTEL-SA-00746 Crypto API Toolkit for Intel SGX Advisory - A potential security vulnerability in the Crypto API Toolkit for Intel SGX (Software Guard Extensions) could allow escalation of privilege. Intel is releasing toolkit updates to mitigate these potential vulnerabilities.
    - CVE-2022-21163 (CVSS base score 8.4) Improper access control in the Crypto API Toolkit for Intel SGX before version 2.0 commit ID 91ee496 could allow an authenticated user to potentially enable escalation of privilege via local access.
- INTEL-SA-00751 Intel QAT Drivers Advisory – This involves potential security vulnerabilities in some Intel QuickAssist Technology (QAT) drivers which could allow escalation of privilege.

Intel is releasing software updates to mitigate these vulnerabilities. For a complete list of Intel's security advisories and additional guidance, click here. HC3 recommends users apply all necessary updates and patches as soon as possible.

Citrix

Citrix released security updates for four high-severity vulnerabilities (CVE-2023-24486, CVE-2023-24484, CVE-2023-24485, and CVE-2023-24483) affecting Citrix Workspace Apps, Virtual Apps and Desktops. If successful, a local threat actor could exploit these vulnerabilities and take control of a compromised system. HC3 recommends users follow CISA's guidance, which encourages users to review Citrix security bulletins for CTX477618, CTX477617, CTX477616 , and apply the necessary patches and updates immediately.

Cisco

Cisco released 23 security advisories to address vulnerabilities in multiple products. Of the advisories listed this month, two have a severity rating of 'Critical,' the highest severity rating possible, and six have a 'High' severity rating. If successful, a remote threat actor could exploit some of these vulnerabilities and take control of a compromised system. CISA encourages users and administrators to review the following advisories:

- ClamAV HFS+ Partition Scanning Buffer Overflow Vulnerability Affecting Cisco Products: February 2023
- Cisco Nexus Dashboard Denial of Service Vulnerability

- Cisco Email Security Appliance and Cisco Secure Email and Web Manager Vulnerabilities

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

VMWare

VMware released 14 security advisories this month. Of these advisories, four were rated 'Critical,' the highest severity rating, five 'Important,' and four were rated as 'Moderate.' Additional information on the critical advisories are as follows:

- VMSA-2023-0004 (CVE-2023-20858 CVSS base score 7.2) - Addresses an injection vulnerability in VMware Carbon Black App.
- VMSA-2022-0004 (CVE-2021-22040, CVE-2021-22041, CVE-2021-22042, CVE-2021-22043, CVE-2021-22050 CVSS base score up to 8.4) - Addresses multiple security vulnerabilities in VMware ESXi, Workstation, and Fusion.
- VMSA-2021-0002 (CVE-2021-21972, CVE-2021-21973, CVE-2021-21974 CVSS base score up to 9.8) - Addresses multiple security vulnerabilities in VMware ESXi and vCenter Server.
- VMSA-2020-0003(CVE-2020-3943, CVE-2020-3944, CVE-2020-3945 CVSS base score up to 9.0)- Addresses multiple security vulnerabilities in vRealize Operations for Horizon Adapter.

For a complete list of VMWare's security advisories, click here. HC3 recommends users follow VMWare's guidance for each and immediately apply patches listed in the 'Fixed Version' column of the 'Response Matrix' that can be accessed by clicking directly on the security advisory.

Fortinet

Fortinet released security updates addressing vulnerabilities affecting numerous products this month. If successful, a threat actor could exploit these flaws and take control of a compromised device or system. HC3 recommends users follow CISA's guidance that "encourages users and administrators to review Fortinet advisories page for additional information," apply all recommended updates and patches immediately. For a complete list of vulnerabilities addressed this month, click here to view FortiGuard Labs' Vulnerability Advisories page.

Adobe

Adobe released security updates addressing numerous vulnerabilities in Adobe software. If successful, a threat actor could exploit these flaws and take control of a compromised system or device.
HC3 recommends following CISA's guidance, which "encourages users and administrators to review the following Adobe Security Bulletins" for the following products:

- After Effects APSB23-02
- Connect APSB23-05
- FrameMaker APSB23-06
- Bridge APSB23-09
- Photoshop APSB23-11

- InDesign APSB23-12
- Premiere Rush APSB23-14
- Animate APSB23-15
- Substance 3D Stager APSB23-16

HC3 also recommends users apply all necessary updates and patches immediately. For a complete list of Adobe security updates, click here.

References

Adobe Plugs Critical Security Holes in Illustrator, After Effects Software
https://www.securityweek.com/adobe-plugs-critical-security-holes-in-illustrator-after-effects-software/

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

Android Security Bulletins
https://source.android.com/security/bulletin

Android Security Bulletin—February 2023
https://source.android.com/docs/security/bulletin/2023-02-01

Android's February 2023 Updates Patch 40 Vulnerabilities
https://www.securityweek.com/androids-february-2023-updates-patch-40-vulnerabilities/

Apple fixes new WebKit zero-day exploited to hack iPhones, Macs
https://www.bleepingcomputer.com/news/security/apple-fixes-new-webkit-zero-day-exploited-to-hack-iphones-macs/

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

Apple Releases Security Updates for Multiple Products
https://www.cisa.gov/news-events/alerts/2023/02/14/apple-releases-security-updates-multiple-products

Cisco Releases Security Advisories for Multiple Products
https://www.cisa.gov/news-events/alerts/2023/02/23/cisco-releases-security-advisories-multiple-products

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

Citrix Releases Security Updates for Workspace Apps, Virtual Apps and Desktops
https://www.cisa.gov/news-events/alerts/2023/02/14/citrix-releases-security-updates-workspace-apps-virtual-apps-and-desktops

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

FortiGuard Labs: February 2023 Vulnerability Advisories
https://www.fortiguard.com/psirt-monthly-advisory/february-2023-vulnerability-advisories

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

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

Microsoft February 2023 Patch Tuesday fixes 3 exploited zero-days, 77 flaws
https://www.bleepingcomputer.com/news/microsoft/microsoft-february-2023-patch-tuesday-fixes-3-exploited-zero-days-77-flaws/

Microsoft fixes three zero-days in its 75-flaw February Patch Tuesday
https://www.zdnet.com/article/microsoft-fixes-three-zero-days-in-its-75-flaw-february-patch-tuesday/

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

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

Mozilla Releases Security Updates for Firefox 110 and Firefox ESR
https://www.cisa.gov/news-events/alerts/2023/02/14/mozilla-releases-security-updates-firefox-110-and-firefox-esr

Mozilla Releases Security Updates for Thunderbird 102.8
https://www.cisa.gov/news-events/alerts/2023/02/17/mozilla-releases-security-updates-thunderbird-1028

Patch Tuesday notes, February 2023
https://thecyberwire.com/stories/82f92b59da464491ae47a22ede97f349/patch-tuesday-notes-february-2023

Pixel Update Bulletin – February 2023
https://source.android.com/docs/security/bulletin/pixel/2023-02-01

SAP Security Notes
https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html

SAP Security Patch Day – February 2023

https://dam.sap.com/mac/app/e/pdf/preview/embed/ucQrx6G?ltr=a&rc=10

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