HC3: Monthly Cybersecurity Vulnerability Bulletin
February 6, 2023 TLP:CLEAR Report: 202302061700

January Vulnerabilities of Interest to the Health Sector

In January 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, 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 5 vulnerabilities in January 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 U.S. 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 fixes for one zero-day vulnerability and 98 flaws. 87 of the 98 vulnerabilities addressed this month have an 'Important' severity rating and 11 are 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:

- 39 Elevation of Privilege Vulnerabilities
- 4 Security Feature Bypass Vulnerabilities
- 33 Remote Code Execution Vulnerabilities
- 10 Information Disclosure Vulnerabilities
- 10 Denial of Service Vulnerabilities
- 2 Spoofing Vulnerabilities

This month's Patch Tuesday also included fixes for one zero-day vulnerability, one actively exploited and a publicly disclosed flaw. Additional information on this actively exploited zero-day vulnerability and other notable vulnerabilities addressed this month are as follows:

- CVE-2023-21674 – *Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability* - This vulnerability is listed as under active exploitation and allows a local threat actor to escalate privileges from sandboxed execution inside Chromium to kernel-level execution and full SYSTEM

privileges. According to researchers, bugs of this type are often paired with some form of code execution to deliver malware or ransomware.

- CVE-2023-21743 - *Microsoft SharePoint Server Security Feature Bypass Vulnerability* - This flaw could allow a remote, unauthenticated threat actor to make an anonymous connection to an affected SharePoint server. It is recommended that systems administrators take additional measures to protect organizations from this vulnerability.
- CVE-2023-21763/CVE-2023-21764 - *Microsoft Exchange Server Elevation of Privilege Vulnerability* – According to researchers, this flaw was discovered as a result of a failed of CVE-2022-41123. If successful, a local threat actor could load their own DLL and execute code at the level of SYSTEM.

For a complete list of Microsoft vulnerabilities released in January 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

There were more than 50 vulnerabilities addressed in Android's security bulletin , affecting devices running Google's Android OS. At the time of release, none one of these vulnerabilities were listed as exploited in the wild. Researchers stated the most serious flaw this month is a high-security vulnerability in the Framework component that could lead to local escalation of privilege with no additional execution privileges required.

Additionally, Google released 17 security fixes and updates including Chrome 109.0.5414.74 (linux),109.0.5414.74/.75(Windows) and 109.0.5414.87(Mac). A list of changes is available in the log and can be viewed by clicking here. Google is reportedly rolling out Chrome 109 to the stable channel for Windows, Mac and Linux soon; more information on this process can be found on Chrome and Chromium blog posts. Google also announced that Chrome support for Windows 7 is coming to an end in February and that Chrome 109 will be the last to support these operating systems. 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
- iOS 12.5.7
- macOS Monterey 12.6.3

- macOS Big Sur 11.7.3
- watchOS 9.3
- iOS 15.7.3 and iPadOS 15.7.3
- iOS 16.3 and iPadOS 16.3
- macOS Ventura 13.2

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 ESR and Firefox. If successful, a threat actor could exploit some of 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 ESR 102.7 and Firefox 109" for additional information and apply necessary patches or updates immediately.

SAP

SAP released 12 new security notes and 3 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. This month, there were seven vulnerabilities with a severity rating of "Hot News", which is the most severe rating. There were also five flaws classified as "Medium" in severity. A breakdown of some security notes for vulnerabilities with a "Hot News" severity rating are as follows:

- Security Note# 3275391 (CVE-2023-0016) has a 9.9 CVSS score and 'Hot News' severity rating. SQL injection vulnerability in SAP Business Planning and Consolidation MS. Product(s) impacted: SAP BPC MS 10.0, Versions – 800, 810.

- Security Note# 3262810– (CVE-2023-0022) has a 9.9 CVSS score and 'Hot News' severity rating. Code Injection vulnerability in SAP BusinessObjects Business Intelligence platform (Analysis edition for OLAP). Product(s) impacted: SAP BusinessObjects Business Intelligence platform (Analysis edition for OLAP), Versions - 420, 430.

- Security Note# 3273480– (CVE-2022-41272) has a 9.9 CVSS score and 'Hot News' severity rating. This is an update to a previous security note that was released in December 2022. Improper access control in SAP NetWeaver Process Integration (User Defined Search). Product(s) impacted: SAP NetWeaver Process Integration, Version – 7.50.

- Security Note# 3243924– (CVE-2022-41203) has a 9.9 CVSS score and 'Hot News' severity rating. This is an update to a previous security note that was released in November 2022. Insecure Deserialization of Untrusted Data in SAP Business Objects Business Intelligence Platform (Central Management Console and BI Launchpad). Product(s) impacted: SAP BusinessObjects Business Intelligence Platform (Central Management Console and BI Launchpad), Versions - 4.2, 4.3.

- Security Note# 3267780– (CVE-2022-41271) has a 9.4 CVSS score and 'Hot News' severity rating. This is an update to a previous security note that was released in December 2022. Improper access control in SAP NetWeaver Process Integration (Messaging System). Product(s) impacted: SAP NetWeaver Process Integration, Version – 7.50.

- Security Note# 3268093 – (CVE-2023-0017) has a 9.4 CVSS score and 'Hot News' severity rating. Improper access control in SAP NetWeaver AS for Java. Product(s) impacted: SAP NetWeaver AS for Java, Version – 7.50.

- Security Note# 3089413 – (CVE-2023-0014) has a 9.0 CVSS score and 'Hot News' severity rating. Capture-replay vulnerability in SAP NetWeaver AS for ABAP and ABAP Platform. Product(s) impacted: SAP NetWeaver ABAP Server and ABAP Platform, Versions - SAP_BASIS 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, KERNEL 7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53, KRNL64NUC 7.22, 7.22EXT.

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 one security center advisory with a high severity rating for their products in January. This advisory provides fixes and workarounds for vulnerabilities that are identified with Intel products. The following is additional on information on this advisory and some notable vulnerabilities addressed:

- INTEL-SA-00773 Intel oneAPI Toolkit software Advisory - Potential security vulnerabilities in some Intel oneAPI Toolkits may allow escalation of privilege. Details on related vulnerabilities and their hyperlinks are as follows:
  - CVE-2022-40196 (CVSS base score 7.8) – Improper access control in the Intel(R) oneAPI DPC++/C++ Compiler before version 2022.2.1 for some Intel(R) oneAPI Toolkits before version 2022.3.1 may allow an authenticated user to potentially enable escalation of privilege via local access.
  - CVE-2022-38136 (CVSS base score 6.7) - Uncontrolled search path in the Intel(R) oneAPI DPC++/C++ Compiler before version 2022.2.1 for some Intel(R) oneAPI Toolkits before version 2022.3.1 may allow an authenticated user to potentially enable escalation of privilege via local access.
  - CVE-2022-41342 (CVSS base score 6.0) - Improper buffer restrictions the Intel(R) C++ Compiler Classic before version 2021.7.1. for some Intel(R) oneAPI Toolkits before version 2022.3.1 may allow a privileged user to potentially enable escalation of privilege via local access.

The affected products above are available for stand-alone download and as part of in the Intel oneAPI Toolkit downloads. HC3 recommends users follow Intel's guidance, which is to update the Intel oneAPI DPC++/C++ Compiler to version 2022.2.1 or later. For a complete list of these updates, click here. 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.

HC3: Monthly Cybersecurity Vulnerability Bulletin
February 6, 2023 TLP:CLEAR Report: 202302061700

Cisco

Cisco released security updates to address vulnerabilities in multiple products for this vendor, including a security advisory for a vulnerability affecting Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME). If successful, a remote threat actor could exploit this vulnerability and cause a denial-of-service condition. 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 one Critical security advisory, which is VMSA-2023-0001.1. This advisory has a maximum VSSv3 base score of 9.8 and impacts VMware vRealize Log Insight. This security advisory addresses the following vulnerabilities: CVE-2022-31706, CVE-2022-31704, CVE-2022-31710, CVE-2022-31711. Additional information on these vulnerabilities are as follows:

- CVE-2022-31706 - The vRealize Log Insight contains a Directory Traversal Vulnerability. An unauthenticated threat actor could inject files into the operating system of an impacted appliance, which could result in remote code execution.
- CVE-2022-31704 - The vRealize Log Insight contains a broken access control vulnerability. An unauthenticated threat actor could inject files into the operating system of an impacted appliance, which could result in remote code execution.
- CVE-2022-31710 - vRealize Log Insight contains a deserialization vulnerability. An unauthenticated threat actor could remotely trigger the deserialization of untrusted data, which could result in a denial of service.
- CVE-2022-31711 - vRealize Log Insight contains an Information Disclosure Vulnerability. A threat actor could remotely collect sensitive session and application information without authentication.

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 a security advisory addressing a vulnerability in several versions of FortiADC. This flaw could allow a remote threat actor "to execute unauthorized code or commands via specifically crafted HTTP requests." HC3 recommends users follow CISA's guidance that "encourages users and administrators to review Fortinet security advisory FG-IR-22-061 " and apply all recommended updates and patches immediately.

Adobe

Adobe released four patches to address 29 vulnerabilities in Adobe Acrobat and Reader, Adobe Dimension, InCopy, and InDesign. The Adobe Reader update provides fixes for 15 vulnerabilities, eight of them are listed as 'Critical' in severity, and if a threat actor is successful, could allow arbitrary code execution if an affected system opened a specially-crafted file. Additionally, patches released addressed

six InDesign flaws, four of which are listed as 'Critical.' A total of six vulnerabilities for Adobe InCopy and two in Dimension were addressed as well. These vulnerabilities could allow arbitrary code execution by a threat actor when a specially prepared file is opened. For a complete list of Adobe security updates, click here. HC3 recommends all users apply necessary updates and patches immediately.

References

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

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

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

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

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

Cisco Releases Security Advisories for Multiple Products
https://www.cisa.gov/uscert/ncas/current-activity/2023/01/20/cisco-releases-security-advisory-unified-cm-and-unified-cm-sme

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

First Patch Tuesday of the year explodes with in-the-wild exploit fix
https://www.theregister.com/2023/01/11/patch_tuesday_january_2023/

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

Fortinet Releases Security Updates for FortiADC
https://www.cisa.gov/uscert/ncas/current-activity/2023/01/04/fortinet-releases-security-updates-fortiadc

Google Pixel Update - January 2023
https://support.google.com/pixelphone/thread/195623748/google-pixel-update-january-2023?hl=en

Intel oneAPI Toolkit software Advisory
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00773.html

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

Microsoft Patch Tuesday, January 2023 Edition
https://krebsonsecurity.com/2023/01/microsoft-patch-tuesday-january-2023-edition/

Microsoft January 2023 Patch Tuesday fixes 98 flaws, 1 zero-day
https://www.bleepingcomputer.com/news/microsoft/microsoft-january-2023-patch-tuesday-fixes-98-flaws-1-zero-day/

Microsoft Patch Tuesday for January 2023 — Snort rules and prominent vulnerabilities
https://blog.talosintelligence.com/microsoft-patch-tuesday-for-january-2023/

Microsoft Patch Tuesday, January 2023 Edition
https://krebsonsecurity.com/2023/01/microsoft-patch-tuesday-january-2023-edition/

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

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

Microsoft Patch Tuesday: 97 Windows Vulns, 1 Exploited Zero-Day
https://www.securityweek.com/microsoft-patch-tuesday-97-windows-vulns-1-exploited-zero-day/

Mozilla Releases Security Updates for Firefox
https://www.cisa.gov/uscert/ncas/current-activity/2023/01/18/mozilla-releases-security-updates-firefox

The January 2023 Security Update Review
https://www.zerodayinitiative.com/blog/2023/1/10/the-january-2023-security-update-review

The January 2023 Patch Tuesday Security Update Review
https://blog.qualys.com/vulnerabilities-threat-research/patch-tuesday/2023/01/10/the-january-2023-patch-tuesday-security-update-review

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

SAP Security Patch Day – January 2023
https://dam.sap.com/mac/app/e/pdf/preview/embed/ucQrx6G?ltr=a&rc=10

SAP Patch Day: January 2023
https://securityboulevard.com/2023/01/sap-patch-day-january-2023/

Stable Channel Update for Desktop https://chromereleases.googleblog.com/2023/01/stable-channel-update-for-desktop.html

Sunsetting support for Windows 7 / 8/8.1 and Windows Server 2012 and 2012 R2 in early 2023

https://support.google.com/chrome/thread/185534985/sunsetting-support-for-windows-7-8-1-in-early-2023?hl=en

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