Office of
Information Security
Securing One HHS

Health Sector Cybersecurity
Coordination Center

HC3: Monthly Cybersecurity Vulnerability Bulletin

April 17, 2023 TLP:CLEAR Report: 202304171200

March Vulnerabilities of Interest to the Health Sector

In March 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, Cisco, 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 18 vulnerabilities in March 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 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 that 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 issued security updates to fix 83 flaws and two actively exploited zero-day vulnerabilities. Nine of these 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:

- 21 Elevation of Privilege Vulnerabilities
- 2 Security Feature Bypass Vulnerabilities
- 27 Remote Code Execution Vulnerabilities
- 15 Information Disclosure Vulnerabilities
- 4 Denial of Service Vulnerabilities
- 10 Spoofing Vulnerabilities
- 1 Edge - Chromium Vulnerability

The count above does not include 21 Microsoft Edge vulnerabilities fixed in the month. March's Patch Tuesday fixes two zero-day vulnerabilities actively exploited in attacks, bringing the total count of vulnerabilities addressed to 101. The two actively exploited zero-day vulnerabilities fixed in today's updates are:

- CVE-2023-23397 - *Microsoft Outlook Elevation of Privilege Vulnerability*: This vulnerability allows specially crafted emails to force a target's device to connect to a remote URL and transmit the Windows account's Net-NTLMv2 hash. According to Microsoft's advisory, "external attackers could send specially crafted emails that will cause a connection from the victim to an external UNC location of attackers' control. This will leak the Net-NTLMv2 hash of the victim to the attacker who can then relay this to another service and authenticate as the victim."
- CVE-2023-24880 - *Windows SmartScreen Security Feature Bypass Vulnerability*: This vulnerability could be used to create executables that bypass the Windows Mark of the Web security warning. According to Microsoft's advisory, with this flaw a threat actor or attacker "can craft a malicious file that would evade Mark of the Web (MOTW) defenses, resulting in a limited loss of integrity and availability of security features such as Protected View in Microsoft Office, which rely on MOTW tagging."

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 60 vulnerabilities and among them, two critical-severity remote code execution (RCE) vulnerabilities impacting Android Systems running versions 11, 12, and 13. Every month, security updates are released in two parts. The first part of the update arrived on devices as a 2023-03-01 security patch level that contains 31 fixes for core Android components like Framework, System, and Google Play. According to Android's security bulletin, a "critical security vulnerability in the System component that could lead to remote code execution with no additional execution privileges needed" is the most severe of these issues because user interaction is not needed for exploitation. The two vulnerabilities are tracked as CVE-2023-20951 and CVE-2023-20954; the remaining 29 flaws addressed for this patch level are high-severity escalation of privilege, information disclosure, and denial of service problems.

The second part of the update arrived on devices as the 2023-02-05 security patch level and contained 29 fixes for the Android Kernel, as well as third-party vendor components from MediaTek, Unisoc, and Qualcomm. The most severe issues addressed with this update are two critical-severity flaws on closed-source Qualcomm components, tracked as CVE-2022-33213 and CVE-2022-33256. The remaining flaws addressed are all high-severity vulnerabilities of undefined type. It is worth noting that Android 10 or older devices have reached the end of life (EoL), and those devices will not receive fixes for the vulnerabilities mentioned. There are, however, some important security fixes that may be able to reach those devices through Google Play system updates. 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 information on the 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 threat actor could 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 the following advisories and apply the necessary updates:

- macOS Ventura 13.3
- Safari 16.4
- Studio Display Firmware Update 16.4
- iOS 15.7.4 and iPadOS 15.7.4
- tvOS 16.4
- macOS Big Sur 11.7.5
- iOS 16.4 and iPadOS 16.4
- macOS Monterey 12.6.4

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 to address vulnerabilities in Firefox 111, Firefox ESR 102.9, and Thunderbird 102.9. 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 111, Firefox ESR 102.9, and Thunderbird 102.9 for more information and apply the necessary updates.

SAP

SAP released 19 new security notes and two 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. In March, there were six with a severity rating of "Hot News," which is the most severe rating. There were also four flaws classified as "High" and 11 as "Medium" in severity. A breakdown of some security notes for vulnerabilities with "Hot News" severity ratings are as follows:

- **Security Note# 3245526** (CVE-2023-25616) has a 9.9 CVSS score. This is a code injection vulnerability in SAP Business Intelligence Platform that could give a threat actor access to resources only available to privileged users. Product(s) impacted: SAP Business Objects Business Intelligence Platform (CMC),Versions–420, 430.
- **Security Note# 3252433** (CVE-2023-23857) has a 9.9 CVSS score. This vulnerability is an Improper Access Control in SAP NetWeaver AS for Java. Due to missing authentication check, SAP NetWeaver AS for Java - version 7.50, allows an unauthenticated threat actor to attach to an open interface and make use of an open naming and directory API to access services which can be used to perform unauthorized operations affecting users and services across systems. Upon successful exploitation, the threat actor will have the ability to read and modify sensitive information. This can

also be used to lock up any element or operation of the system making it unresponsive or unavailable. Product(s) impacted: SAP NetWeaver AS for Java, Version –7.50.

- **Security Note# 3294595** (CVE-2023-27269) has a 9.6 CVSS score. This is a directory traversal problem in SAP NetWeaver Application Server for ABAP and ABAP Platform that allows a non-admin user or threat actor to overwrite system files. Product(s) impacted: SAP NetWeaver Application Server for ABAP and ABAP Platform, Versions -700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757,791.
- **Security Note# 3302162** (CVE-2023-27500) has a 9.6 CVSS score. This is a directory traversal vulnerability in SAP NetWeaver Application Server for ABAP and ABAP Platform(SAPRSBRO Program). If successful, a threat actor could exploit this vulnerability in SAPRSBRO to overwrite system files, causing damage to the vulnerable endpoint. Product(s) impacted: SAP NetWeaver AS for ABAP and ABAP Platform (SAPRSBRO Program), Versions –700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757.
- **Security Note# 3283438** (CVE-2023-25617) has a 9.0 CVSS score. This is an OS command execution vulnerability in SAP Business Objects Business Intelligence Platform(Adaptive Job Server). If successful, a remote threat actor could exploit this flaw to execute arbitrary commands on the OS using the BI Launchpad, Central Management Console, or a custom application based on the public java SDK, under certain conditions. Product(s) impacted: SAP Business Objects (Adaptive Job Server), Versions –420,430.

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.

Cisco

Cisco released 28 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 11 have a 'High' severity rating. If successful, a remote threat actor could exploit some of these vulnerabilities and take control of a compromised system. HC3 recommends following CISA's guidance that encourages users and administrators to review the following advisories and apply the necessary updates:

- Cisco IOS XE Software Virtual Fragmentation Reassembly Denial of Service Vulnerability
- Cisco IOS XE Software IOx Application Hosting Environment Privilege Escalation Vulnerability
- Cisco IOS XE SD-WAN Software Command Injection Vulnerability
- Cisco IOS XE Software Fragmented Tunnel Protocol Packet Denial of Service Vulnerability
- Cisco IOS and IOS XE Software IPv6 DHCP (DHCPv6) Relay and Server Denial of Service Vulnerability
- Cisco IOS XE Software for Wireless LAN Controllers HTTP Client Profiling Denial of Service Vulnerability
- Cisco DNA Center Privilege Escalation Vulnerability
- Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches Secure Boot Bypass

- Cisco Access Point Software Association Request Denial of Service Vulnerability

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.

Fortinet

Fortinet released security updates addressing vulnerabilities affecting numerous products for March. If successful with their attack, 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's March 2023 Vulnerability Advisories page for additional information, and 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

For Path Tuesday, 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:

- Commerce APSB23-17
- Experience Manager APSB23-18
- Illustrator APSB23-19
- Dimension APSB23-20
- Creative Cloud Desktop Application APSB23-21
- Substance 3D Stager APSB23-22
- Photoshop APSB23-23
- ColdFusion APSB23-25

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

References

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

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

Android Security Bulletin—March 2023
https://source.android.com/docs/security/bulletin/2023-03-01

Apple Releases Security Updates for Multiple Products https://www.cisa.gov/news-events/alerts/2023/03/28/apple-releases-security-updates-multiple-products

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

CISA Fortinet Releases March 2023 Vulnerability Advisories
https://www.cisa.gov/news-events/alerts/2023/03/09/fortinet-releases-march-2023-vulnerability-advisories

Cisco Releases Security Advisories for Multiple Products
https://www.cisa.gov/news-events/alerts/2023/03/23/cisco-releases-security-advisories-multiple-products

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

Dangerous Android phone 0-day bugs revealed – patch or work around them now!
https://nakedsecurity.sophos.com/2023/03/17/dangerous-android-phone-0-day-bugs-revealed-patch-or-work-around-them-now/

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

Fortinet: New FortiOS bug used as zero-day to attack govt networks
https://www.bleepingcomputer.com/news/security/fortinet-new-fortios-bug-used-as-zero-day-to-attack-govt-networks/

Fortinet Zero-Day and Custom Malware Used by Suspected Chinese Actor in Espionage Operation
https://www.mandiant.com/resources/blog/fortinet-malware-ecosystem

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

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

Microsoft March 2023 Patch Tuesday fixes 2 zero-days, 83 flaws
https://www.bleepingcomputer.com/news/microsoft/microsoft-march-2023-patch-tuesday-fixes-2-zero-days-83-flaws/

March 2023 Vulnerability Advisories
https://www.fortiguard.com/psirt-monthly-advisory/march-2023-vulnerability-advisories

SAP releases security updates fixing five critical vulnerabilities
https://www.bleepingcomputer.com/news/security/sap-releases-security-updates-fixing-five-critical-

vulnerabilities/

SAP Releases Five 'Hot News' Notes on March 2023 Patch Day
https://www.securityweek.com/sap-releases-five-hot-news-notes-on-march-2023-patch-day/

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

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

The March 2023 Patch Tuesday Security Update Review
https://blog.qualys.com/vulnerabilities-threat-research/patch-tuesday/2023/03/14/the-march-2023-patch-tuesday-security-update-review

The March 2023 Security Update Review
https://www.zerodayinitiative.com/blog/2023/3/14/the-march-2023-security-update-review

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