HC3: Monthly Cybersecurity Vulnerability Bulletin
March 19, 2024 TLP:CLEAR Report: 202403191500

February Vulnerabilities of Interest to the Health Sector

In February 2024, 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 February are from Ivanti, ConnectWise, Microsoft, Google/Android, Apple, Mozilla, Cisco, SAP, VMWare, Adobe, Fortinet, and Atlassian. A vulnerability is given the classification of a zero-day when it is actively exploited with no fix available or if it is publicly disclosed. HC3 recommends patching all vulnerabilities, with special consideration given 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 9 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 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 the vulnerabilities in this catalog and consider prioritizing them as part of their risk mitigation plan. The full database can be found here.

Ivanti

Ivanti released a security update regarding the Ivanti Connect Secure and Ivanti Policy Secure Gateways, which gained a lot of attention in January. Additionally, CISA released a joint advisory on threat actors exploiting these vulnerabilities. According to the advisory, cyber threat actors have exploited flaws in Connect Secure and Policy Secure, which are tracked as CVE-2024-46805, CVE-2024-21887, and CVE-2024-21893, where the threat actors can exploit a chain to bypass authentication, craft malicious requests, and execute arbitrary commands with elevated privileges. CISA also relayed the following two key findings:

- The Ivanti Integrity Checker Tool is not sufficient to detect compromise due to the ability of threat actors to deceive it, and
- A cyber threat actor may be able to gain root-level persistence despite the victim having issued factory resets on the Ivanti device.

Additional information on the previously mentioned vulnerabilities can be found below:

- CVE-2023-46805: An authentication bypass vulnerability in the web component of Ivanti ICS 9.x, 22.x and Ivanti Policy Secure allows a remote attacker to access restricted resources by bypassing control checks.
- CVE-2024-21887: A command injection vulnerability in web components of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows an authenticated administrator to send specially crafted requests and execute arbitrary commands on the appliance.

- CVE-2024-21888: This vulnerability is a privilege escalation in the web component of Connect Secure and Policy Secure and can allow a user obtain administrator privileges.

HC3 strongly encourages all users to follow the manufacturers and CISA's guidance and to apply any necessary updates or mitigations to prevent serious damage from occurring to the HPH sector. The full alert from Ivanti can be viewed here.

ConnectWise

ConnectWise disclosed a vulnerability in ScreenConnect, a remote desktop software application, which malicious actors and ransomware operators have actively exploited to gain unauthorized access into affected devices. The vulnerabilities are tracked as CVE-2024-1708 and CVE-2024-1709, and affect versions 23.9.7 and prior. Additionally, CVE-2024-1709 was added to CISA's Known Exploited Vulnerabilities Catalog due to active exploitation. HC3 recommends that all users review the security alert from ConnectWise to prevent serious damage from occurring the Health and Public Health Sector.

Additional Information on these vulnerabilities can be found below:

- CVE-2024-1708: This is a path-traversal vulnerability that can allow a remote actor the ability to execute remote code, or directly impact confidential data and critical systems.
- CVE-2024-1709: This is an Authentication Bypass Using an Alternate Path or Channel vulnerability that may allow for an attacker access to confidential information.

Microsoft

Microsoft released or provided security updates for 73 vulnerabilities. It was reported that there were two actively exploited or publicly disclosed vulnerabilities. Six of these vulnerabilities were rated as critical in severity. Microsoft has also reported on six non-Microsoft CVEs in their February release notes, which impacts Chrome. Additional information on the critical vulnerabilities from the national vulnerability database can be found below:

- CVE-2024-21364: Microsoft Azure Site Recovery Elevation of Privilege Vulnerability
- CVE-2024-21376: Microsoft Azure Kubernetes Service Confidential Container Remote Code Execution Vulnerability
- CVE-2024-21401: Microsoft Entra Jira Single-Sign-On Plugin Elevation of Privilege Vulnerability
- CVE-2024-21403: Microsoft Azure Kubernetes Service Confidential Container Elevation of Privilege Vulnerability
- CVE-2024-21410: Microsoft Exchange Server Elevation of Privilege Vulnerability
- CVE-2024-21413: Microsoft Outlook Remote Code Execution Vulnerability

For a complete list of Microsoft vulnerabilities and security updates, click here. HC3 recommends that all users follow Microsoft's guidance 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/Android released two updates in early February. The first update was released on February 01, 2024 and addressed nine vulnerabilities in the Framework and System components. One of these

vulnerabilities was given a critical rating, and the remaining were rated as high in severity, and according to Google, "the most severe vulnerability in this section could lead to local escalation of privilege with no additional execution privileges needed." The critical vulnerability is tracked as CVE-2024-0031 and impacts versions 11, 12, 12L, 13, and 14 of Android. The second part of Google's/Android's security advisory was released on February 05, 2024, and it addressed updates in the Arm, MediaTek, Unisoc Components, Qualcomm components, and Qualcomm closed-source components. All vulnerabilities were rated as high in severity.

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 improves 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, and the chrome browser update, can be viewed here.

Apple

Apple released multiple security updates in February, for several different products. HC3 recommends reviewing the Apple security updates and Rapid Security Responses for the following:

- visionOS 1.0.3
- Safari 17.3.1
- iOS 17.3.1 and iPadOS 17.3.1
- macOS Sonoma 14.3.1
- watchOS 10.3.1

There were no alerts from CISA regarding Apple devices this month. For a complete list of the latest Apple security and software updates, click here. HC3 recommends that 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 security advisories in February addressing vulnerabilities affecting Firefox, Firefox ESR, and Thunderbird. All three of the vulnerabilities were rated as high in severity and if successful, a threat actor could exploit these vulnerabilities to take control of a compromised system or device. HC3 encourages all users to follows CISA's guidance to review the following advisories and apply the necessary updates:

- Firefox 123
- Firefox ESR 115.8
- Thunderbird 115.8

A complete list of Mozilla's updates including lower severity vulnerabilities are available on the Mozilla Foundation Security Advisories page. HC3 recommends applying the necessary updates and patches immediately, and following Mozilla's guidance for additional support.

Cisco

Cisco released 13 security updates to address vulnerabilities in multiple products. Two of the vulnerabilities were classified as "Critical" in severity, five as "High," and the remaining were classified as "Medium" in severity. The critical vulnerabilities impact Cisco Expressway Series (CVE-2024-20252, CVE-

2024-20254, CVE-2024-20255) and Unity Connection products (CVE-2024-20272). Additionally, CISA released a security advisory warning about Cisco Expressway and reported that "a threat actor could exploit this vulnerability to take control of an affected system." Additional information on the critical vulnerabilities addressed by Cisco can be found below:

- CVE-2024-20252, CVE-2024-20254, CVE-2024-20255: There are multiple vulnerabilities in Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) which could allow an unauthenticated, remote attacker to conduct cross-site request forgery (CSRF) attacks and perform arbitrary actions on an affected device.
- CVE-2024-20272: A vulnerability in the web-based management interface of Cisco Unity Connection could allow an unauthenticated, remote attacker to upload arbitrary files to an affected system and execute commands on the underlying operating system.

For a complete list of Cisco security advisories released in February, 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.

SAP

SAP released 13 security notes and three updates to previously issued security notes, to address vulnerabilities affecting multiple products. If successful in launching an attack, a threat actor could exploit these vulnerabilities and take control of a compromised device or system. This month there were two vulnerabilities with a severity rating of "Hot News", which is the most severe and a top priority for SAP. The remaining flaws consisted of six "High", seven "Medium", and one "Low" rated vulnerability in severity. A breakdown of the Hot News security notes for the month of February can be found below:

- **Security Note #2622660** (No associated CVE): This is an update to a security note released in April 2018 for the browser control Google Chromium delivered with SAP Business Client.
- **Security Note #3420923** (CVE-2024-22131): This vulnerability was given a CVSS score of 9.1 and it is code injection vulnerability in SAP ABA (Application Basis) in versions - 700, 701, 702, 731, 740, 750, 751, 752, 75C, 75I.

For a complete list of SAP's security notes and updates for vulnerabilities released in February, 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.

VMWare

VMWare released one critical security advisory update, which addresses multiple vulnerabilities in VMware Enhanced Authentication Plug-in (EAP). Additional information on this vulnerability is listed below:

- VMSA-2024-0003 (CVE-2024-22245, CVE-2024-22250): Arbitrary Authentication Relay and Session Hijack vulnerabilities in the deprecated VMware Enhanced Authentication Plug-in (EAP)

For a complete list of VMWare's security advisories, click here. Patches are available to remediate these vulnerabilities found in VMWare products. To remediate the listed vulnerabilities, apply the updates listed in the 'Fixed Version' column of the 'Response Matrix' below to affected deployments. HC3 recommends

that users follow VMWare's guidance for each, and apply patches listed in the 'Fixed Version' column of the 'Response Matrix', which can be accessed by clicking directly on the security advisory.

Adobe

Adobe released multiple security advisories for different products. HC3 recommends that all users follow CISA's guidance to review the following bulletins and apply the necessary updates and patches immediately.

- Adobe Commerce and Magento
- Adobe Substance 3D Painter
- Adobe Acrobat and Reader
- Adobe FrameMaker Publishing Server
- Adobe Audition
- Adobe Substance 3D Designer

Fortinet

Fortinet's February vulnerability advisory addressed two critical vulnerabilities in FortiOS. The vulnerabilities are tracked as CVE-2024-21762 and CVE-2024-23113. CVE-2024-21762 is an out of bounds write which exists in multiple versions of FortiOS. CVE-2024-23113, according to Fortinet, "is a use of externally-controlled format string vulnerability in FortiOS fgfmd daemon, which may allow a remote unauthenticated attacker to execute arbitrary code or commands." If successful, a threat actor can exploit this vulnerability and take control of a compromised device or system. HC3 recommends that all users review Fortinet's Vulnerability Advisory page, and apply all necessary updates and patches immediately:

- FG-IR-24-015
- FG-IR-24-029

Atlassian

Atlassian released a security advisory regarding eleven high-severity vulnerabilities in their February 2024 Security Bulletin. All vulnerabilities were rated as high in severity. The highest was rated as an 8.5 on the CVSS scale and is tracked as CVE-2024-21678. CVE-2024-21678 is described as a Stored XSS vulnerability, which was introduced in version 2.7.0 of Confluence Data Center, and it can allow for an unauthenticated remote attacker to execute arbitrary HTML or JavaScript code on a victim's browser.

A complete list of security advisories and bulletins from Atlassian can be viewed here. HC3 recommends that all users apply necessary updates and patches immediately.

References

Adobe Security Updates
Adobe Product Security Incident Response Team (PSIRT)

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

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

Atlassian Security Bulletin
Security Advisories | Atlassian

CISA and Partners Release Advisory on Threat Actors Exploiting Ivanti Connect Secure and Policy Secure Gateways Vulnerabilities
https://www.cisa.gov/news-events/alerts/2024/02/29/cisa-and-partners-release-advisory-threat-actors-exploiting-ivanti-connect-secure-and-policy-secure

CISA Adds One Known Exploited ConnectWise Vulnerability, CVE-2024-1709, to Catalog
https://www.cisa.gov/news-events/alerts/2024/02/22/cisa-adds-one-known-exploited-connectwise-vulnerability-cve-2024-1709-catalog

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

ConnectWise ScreenConnect 23.9.8 security fix
https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8

Fortinet PSIRT Advisories
PSIRT Advisories | FortiGuard

Ivanti Connect Secure and Ivanti Policy Secure Gateways Alert
CVE-2023-46805 (Authentication Bypass) & CVE-2024-21887 (Command Injection) for Ivanti Connect Secure and Ivanti Policy Secure Gateways

KB CVE-2023-46805 (Authentication Bypass) & CVE-2024-21887 (Command Injection) for Ivanti Connect Secure and Ivanti Policy Secure Gateways
https://forums.ivanti.com/s/article/KB-CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US

Microsoft February 2024 Patch Tuesday fixes 2 zero-days, 73 flaws
https://www.bleepingcomputer.com/news/microsoft/microsoft-february-2024-patch-tuesday-fixes-2-zero-days-73-flaws/#google_vignette

Microsoft February 2024 Patch Tuesday
https://isc.sans.edu/diary/Microsoft+February+2024+Patch+Tuesday/30646

Microsoft Month Archives: February 2024
2024/02 | Microsoft Security Response Center

Mozilla Foundation Security Advisory 2024-05
https://www.mozilla.org/en-US/security/advisories/mfsa2024-05/

Mozilla Foundation Security Advisory 2024-06
https://www.mozilla.org/en-US/security/advisories/mfsa2024-06/

Mozilla Foundation Security Advisory 2024-07

https://www.mozilla.org/en-US/security/advisories/mfsa2024-07/

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

Mozilla Foundation Security Advisories
https://www.mozilla.org/en-US/security/advisories/

SAP Security Patch Day – February 2024
SAP Security Patch Day – February 2024

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

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