Office of
Information Security
Securing One HHS

Health Sector Cybersecurity
Coordination Center

HC3: Monthly Cybersecurity Vulnerability Bulletin

February 05, 2024 TLP:CLEAR Report: 202402051700

January Vulnerabilities of Interest to the Health Sector

In January 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 January are from Ivanti, Microsoft, Google/Android, Apple, Mozilla, Cisco, SAP, VMWare, Adobe, Fortinet, Atlassian, and Jenkins. 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 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 21 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 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 which addressed an authentication bypass vulnerability (CVE-2023-46805) along with a command injection vulnerability (CVE-2024-21887) that impacts the Connect Secure and Policy Secure gateways. In the report, Ivanti noted that both vulnerabilities were under active exploitation. Towards the end of January, CISA released an Emergency Directive for Federal Civilian Executive Branch agencies to implement mitigations and apply updates within 48 hours of Ivanti releasing updates. On January 30, 2024, CISA released an alert on New Mitigations to Defend Against Exploitation of Ivanti Connect Secure and Policy Secure Gateways. Additional information on these 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.

At the end of January, Ivanti released an updated security advisory warning of two new zero-days which are tracked as CVE-2024-21888, which is a privilege escalation vulnerability. Along with CVE-2024-21893, a server-side request forgery vulnerability in SAML of Ivanti Connect Secure. According to Ivanti: "At the time of publication, the exploitation of CVE-2024-21893 appears to be targeted. Ivanti expects the threat actor to change their behavior and we expect a sharp increase in exploitation once this information is public."

HC3 strongly encourages all users to follow the manufacturer's 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.

Microsoft

Microsoft released or provided security updates for 48 vulnerabilities. It was reported that there were not any actively exploited or publicly disclosed vulnerabilities. Two of these vulnerabilities were rated as critical in severity and are tracked as CVE-2024-0057 and CVE-2024-20674. Microsoft has also reported on five non-Microsoft CVEs in their January release notes, which impacts Chrome and a vulnerability in SQLite. Additional information on the critical vulnerabilities can be found below:

- CVE-2023-0057 (CVSS score: 9.1): Improper Restriction of Rendered UI Layers or Frames in GitHub repository pyload/pyload prior to 0.5.0b3.dev33.
- CVE-2024-20674 (CVSS score: 9.0): Windows Kerberos Security Feature Bypass Vulnerability

For a complete list of Microsoft vulnerabilities and security updates, click here. HC3 recommends that 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/Android released two updates in early January. The first update was released on January 01, 2024 and addressed 10 vulnerabilities in the Framework and System components. All ten of these vulnerabilities were rated as high in severity and according to Google, "the most severe of these issues is a high security vulnerability in the Framework component that could lead to local escalation of privilege with no additional execution privileges needed." The vulnerability is tracked as CVE-2023-21245 and impacts versions 11, 12, 12L, 13, and 14 of Android. The second part of Google/Android's January security advisory was released on January 05, 2024, and it addressed updates in the Arm, Imagination Technologies, MediaTek, Unisoc Components, Qualcomm components, and Qualcomm closed-source components. Three of the vulnerabilities in the Qualcomm closed-source components were rated as critical in severity, and the remaining were given a high classification in severity. Information on the critical vulnerabilities can be found below:

- CVE-2023-21651: In this vulnerability, there is a memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE.
- CVE-2023-33025: In this vulnerability, there is a memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call.
- CVE-2023-33036: This vulnerability is a permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call.

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, along with security information on vulnerabilities for the month of December, can be viewed by clicking here, and the Chrome browser update can be viewed here.

Apple

Apple released multiple security updates in January, for several different products. HC3 recommends following CISA guidance "which encourages users and administrators to review the following advisories and apply necessary updates":

- iOS 17.3 and iPadOS 17.3
- iOS 16.7.5 and iPadOS 16.7.5
- iOS 15.8.1 and iPad 15.8.1
- macOS Sonoma 14.3
- macOS Ventura 13.6.4
- macOS Monterey 12.7.3
- Safari 17.3
- watchOS 10.3
- tvOS 17.3

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 January addressing vulnerabilities affecting Firefox 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 122
- Firefox ESR 115.7
- Thunderbird 115.7

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 17 security updates to address vulnerabilities in multiple products. Two of the vulnerabilities were classified as critical in severity, three as high, and the remaining were classified as medium in severity. The critical vulnerabilities impact Cisco Unified Communications and Contract Center Solutions products (CVE-2024-20253) and Cisco Unity Connect (CVE-2024-20272). Additionally, CISA released a security advisory warning about CVE-2024-20272 and reported that "a threat actor could exploit this vulnerability to take control of an affected system." The following contains additional information on the critical vulnerabilities addressed by Cisco:

- CVE-2024-20253: A vulnerability in the command line interface (cli) management interface of Cisco SD-WAN vManage could allow an authenticated, local attacker to bypass authorization and allow the attacker to roll back the configuration on vManage controllers and edge router 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 January, 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 ten security notes and two 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 three vulnerabilities with a severity rating of “Hot News”, which is the most severe and a top priority for SAP. The remaining flaws consisted of four high, four medium, and one low rated vulnerability in severity. A breakdown of the Hot News security notes for the month of January can be found below:

- **Security Note #3412456** (CVE-2023-49583): This vulnerability is an escalation of privileges in applications developed through SAP Business Application Studio, SAP Web IDE Full-Stack and SAP Web IDE for SAP HANA
- **Security Note #3413475** (CVE-2023-49583, CVE-2023-50422): This vulnerability was given a CVSS score of 9.1 and it is an escalation of privileges flaw in the SAP Edge Integration Cell.
- **Security Note #3411067** (CVE-2023-49583, CVE-2023-50422, CVE-2023-50423, CVE-2023-50424)**:** This vulnerability was given a CVSS score of 9.1 and it is an update to Security Note released in December 2023 and it is an escalation privileges flaw in SAP Business Technology Platform (BTP) Security Services Integration Libraries.

For a complete list of SAP’s security notes and updates for vulnerabilities released in January, 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 that addresses a missing access control vulnerability in VMware Aria Automation. Additional information on this vulnerability is listed below:

- VMSA-2024-0001 (CVE-2023-34063): Aria Automation contains a Missing Access Control vulnerability. An authenticated malicious actor may exploit this vulnerability, leading to unauthorized access to remote organizations and workflows.

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

Adobe

Adobe released one security advisory which addressed six vulnerabilities in Adobe Substance 3D Stager. This vulnerability has not been reported to be exploited in the wild; however, successful exploitation could lead to memory leaks and remote code execution. For a complete list of Adobe security updates, click here. HC3 recommends that all users apply necessary updates and patches immediately.

- Adobe Substance 3D Stager

Fortinet

Fortinet's January vulnerability advisory addressed vulnerabilities in FortiOS and FortiProxy software. The advisory came with a high rating in severity, with a CVSS score of 8.3 and is being tracked as CVE-2023-44250. This vulnerability can allow an authenticated attacker to perform elevated actions through crafted HTTP/HTTPS request. 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-23-315

Atlassian

Atlassian released a security advisory regarding 28 high-severity vulnerabilities in their January 2024 Security Bulletin. The two highest critical vulnerabilities were both rated as an 8.8 on the CVSS scale and can result in remote code execution. These vulnerabilities are tracked as CVE-2020-26217 and CVE-2018-10054. Additionally, CISA released an advisory regarding a security alert from Atlassian on CVE-2023-22527 that impacts out-of-date versions of Confluence Data Center and Server, stating that "malicious cyber actor could exploit one of these vulnerabilities to take control of an affected system." Additional information on this vulnerability can be found below:

- Atlassian Confluence Vulnerability

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.

Jenkins

In late January, Jenkins, an open-source automation server for continuous integration and continuous development (CI/CD), released a security advisory for CVE-2024-23897. This vulnerability impacts the following plugins:

- Jenkins (core)
- Git Server Plugin
- GitLab Branch Source Plugin
- Log Command Plugin
- Matrix Project Plugin
- Qualys Policy Compliance Scanning Connector Plugin
- Red Hat Dependency Analytics Plugin

According to Jenkins: "Jenkins has a built-in command line interface (CLI) to access Jenkins from a script or shell environment. Jenkins uses the args4j library to parse command arguments and options on the Jenkins controller when processing CLI commands. This command parser has a feature that replaces an @ character followed by a file path in an argument with the file's contents (expandAtFiles). This feature is enabled by default and Jenkins 2.441 and earlier, LTS 2.426.2 and earlier does not disable it. This allows attackers to read arbitrary files on the Jenkins controller file system using the default character encoding of the Jenkins controller process." Reports from ShadowServer indicate that approximately 45,000 instances of this are publicly exposed. HC3 strongly encourages all users to adhere to the mitigations found the Jenkins security advisory above to prevent serious damage from occurring to the HPH sector.

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 Releases Security Advisories for Multiple Products
https://www.cisa.gov/news-events/alerts/2024/01/18/atlassian-releases-security-updates-multiple-products

Atlassian Security Bulletin – January 16 2024
Security Bulletin - January 16 2024 | Atlassian Support | Atlassian Documentation

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

VMware Security Advisories
https://www.vmware.com/security/advisories.html

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

Jenkins Security Advisory 2024-01-24
Jenkins Security Advisory 2024-01-24

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

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

ShadowServer General Statistics World Map
World map · General statistics · The Shadowserver Foundation

Microsoft January 2024 Patch Tuesday fixes 49 flaws, 12 RCE bugs
https://www.bleepingcomputer.com/news/microsoft/microsoft-january-2024-patch-tuesday-fixes-49-flaws-12-rce-bugs/

Microsoft January 2024 Patch Tuesday
Microsoft January 2024 Patch Tuesday - SANS Internet Storm Center

Microsoft Month Archives: January 2024
2024/01 | Microsoft Security Response Center

Mozilla Foundation Security Advisory 2024-01
Security Vulnerabilities fixed in Firefox 122 — Mozilla

Mozilla Foundation Security Advisory 2024-02
Security Vulnerabilities fixed in Firefox ESR 115.7 — Mozilla

Mozilla Foundation Security Advisory 2024-04
Security Vulnerabilities fixed in Firefox ESR 115.7 — Mozilla

Mozilla Releases Security Updates for Thunderbird and Firefox
https://www.cisa.gov/news-events/alerts/2024/01/24/mozilla-releases-security-updates-thunderbird-and-firefox

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

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

New Mitigations to Defend Against Exploitation of Ivanti Connect Secure and Policy Secure Gateways
New Mitigations to Defend Against Exploitation of Ivanti Connect Secure and Policy Secure Gateways | CISA

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