Office of
Information Security
Securing One HHS

Health Sector Cybersecurity
Coordination Center

# HC3: Monthly Cybersecurity Vulnerability Bulletin

January 04, 2024 TLP:CLEAR Report: 202401041700

## December Vulnerabilities of Interest to the Health Sector

In December 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 December are from 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 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 11 vulnerabilities in December 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.

### Microsoft

Microsoft released or provided security updates for 37 vulnerabilities, including one previously disclosed zero-day from August that was patched. Two of these vulnerabilities were listed as critical. The previously disclosed zero-day is tracked as CVE-2023-20588, which is a division-by-zero bug in AMD processors and can result in the compromise of sensitive data. Additional information on the critical vulnerabilities can be found below:

- CVE-2023-35618 (CVSS score: 9.6): Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability.
- CVE-2023-36019 (CVSS score: 9.6): Microsoft Power Platform Connector Spoofing 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 early in December which addressed 94 vulnerabilities. Three of these vulnerabilities were rated as critical in severity, and the remaining were rated as high. According to Google, "The most severe of these issues is a critical security vulnerability in the System component that could lead to remote (proximal/adjacent) code execution with no additional execution privileges needed.

User interaction is not needed for exploitation." The vulnerability is tracked as CVE-2023-40088 and impacts versions 11, 12, 12L, 13, and 14 of Android. The second part of Google/Androids' December security advisory addressed updates in the Arm, Imagination Technologies, MediaTek, Misc OEM, Unisoc Components, and Qualcomm components, with an additional critical vulnerability identified in the Qualcomm closed-source component. Information on the critical vulnerabilities can be found below:

- CVE-2023-40077: In this vulnerability, there is a possible UAF write due to a race condition in multiple functions of MetaDataBase.cpp. This could lead to a remote escalation of privilege without requiring user interaction.
- CVE-2023-40076: In this vulnerability, it is a possible to access credentials from other users due to a permissions bypass in the createPendingIntent of CredentialManagerUi.java. This could lead to local escalation of privileges with no additional execution privileges needed. User interaction is also not needed for this vulnerability.
- CVE-2022-40507: This vulnerability is a memory corruption resulting from double free in Core while mapping HLOS (High Level Operating System) address to the list.

Additionally, Google reported that indications that the following may be under limited, targeted exploitation: CVE-2023-33063, CVE-2023-3310, CVE-2023-33106. HC3 recommends users refer to the Android and Google service mitigations section for a summary of the mitigations provided by the 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 December, for several different products. HC3 recommends following CISA's guidance, which encourages users and administrators to review the following advisories and apply necessary updates:

- Safari 17.1.2
- macOS Sonoma 14.1.2
- iOS 17.1.2 and iPad 17.1.2
- Safari 17.2
- iOS 17.2 and iPadOS 17.2
- iOS 16.7.3 and iPad 16.7.3
- macOS Sonoma 14.2
- macOS Ventura 13.6.3
- macOS Monterey 12.7.2

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 December 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 121
- Firefox ESR 115.6
- Thunderbird 155.6

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 three security updates to address vulnerabilities in multiple products. One of the vulnerabilities was classified as critical in severity, one as high, and the remaining vulnerability was classified as medium in severity. The critical vulnerability involves Apache Struts and impacts the Identity Service Engine (ISE), which is tracked as CVE-2023-50164. Through this vulnerability, a threat actor can manipulate file upload params to conduct path traversal. Additionally, under some circumstances this can also lead to uploading malicious files, which can be leveraged to perform remote code execution. Additional information on this vulnerability can also be view at the Apache Software Security Bulletin. The following versions of Apache Struts are impacted by this vulnerability:

- 2.0.0 through 2.5.32
- 6.0.0 through 6.3.0.1
- 2.0.0 through 2.3.37 (no longer supported)

For a complete list of Cisco security advisories released in December, 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 fourteen 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 four 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”, seven “Medium”, and two “Low” rated vulnerabilities in severity. A breakdown of the Hot News security notes for the month of December can be found below:

- **Security Note #2622660** (No listed CVE): This vulnerability was given a CVSS score of 10.0 and it is an update for the browser control Google Chromium delivered with the SAP Business Client.
- **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 escalation of privileges flaw in the SAP Business Technology Platform.
- **Security Note #3399691** (CVE-2023-36922**):** This vulnerability was given a CVSS score of 9.1 and it is an update to Security Note #3350297, which can result in an OS Command Injection vulnerability in SAP ECC and SAP S/4HANA (IS-OIL).

- **Security Note #3350297** (CVE-2023-36922): This vulnerability was given a CVSS score of 9.1 and it is an update to a released note from July 2023, which can lead to an OS Command Injection vulnerability in SAP ECC and SAP S/4HANA (IS-OIL).

For a complete list of SAP's security notes and updates for vulnerabilities released in December, click here. HC3 recommends patching immediately and following SAP's guidance for additional support. To fix vulnerabilities discovered in SAP products, SAP recommends that customers visit the Support Portal and apply patches to protect their SAP landscape.

## VMWare

VMWare released one moderate security advisory update regarding a privilege escalation in the VMware Workspace ONE Launcher. Additional information on this vulnerability is listed below:

- VMSA-2023-0027 (CVE-2023-34064): Through this vulnerability, an attacker with physical access to the Workspace ONE Launcher could exploit the edge panel feature to bypass the setup and gain access to sensitive information.

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' that can be accessed by clicking directly on the security advisory.

## Adobe

Adobe released security advisories to address multiple critical and important vulnerabilities in Adobe software. If successful, a threat actor could exploit some of these vulnerabilities to escalate their privileges or conduct arbitrary code execution. HC3 recommends that all users review the Adobe Security Bulletins and follow CISA's guidance, which encourages users and administrators to review the following advisories and apply the necessary updates:

- Adobe Prelude
- Adobe Illustrator
- Adobe InDesign
- Adobe Dimension
- Adobe Substance3D Designer
- Adobe Experience Manager
- Adobe Substance3D Stager
- Adobe Substance3D Sampler
- Adobe Substance3D After Effects

Additionally in December, CISA released a security advisory warning of threat actors exploiting CVE-2023-2630. CVE-2023-2630 is a vulnerability in Adobe ColdFusion, which can lead to improper access control and result in arbitrary code execution. This vulnerability is reported to have been used for gaining initial access into government servers. For a complete list of Adobe security updates, click here. HC3 recommends that all users apply necessary updates and patches immediately.

## Fortinet

Fortinet's December vulnerability advisory addressed several vulnerabilities across different Fortinet products. The advisories all came with a high rating in severity. The highest was rated with a CVSS score of

8.3 and is tracked as CVE-2023-41678. This vulnerability is a double free vulnerability in FortiOS and FortiPAM HTTPSd daemon, and can result in the unauthorized execution of codes 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-23-196
- FG-IR-22-038
- FG-IR-23-138

## Atlassian

Atlassian released a security advisory regarding four critical and seven high-severity vulnerabilities in their December 2023 Security Bulletin. The two highest critical vulnerabilities were both rated as a 9.8 on the CVSS scale and can result in remote code execution. These vulnerabilities are tracked as CVE-2023-22524 and CVE-2022-1471. All the vulnerabilities that were rated as "High" in severity were given a CVSS score of 7.5. Additional details of the four critical vulnerabilities can be found below, and a security advisory from CISA on these can be accessed here.

- CVE-2023-22522: This vulnerability is a template injection which can allow an authenticated attacker to inject malicious user input into a Confluence page, which could enable an attacker to achieve remote code execution on the affected instance.
- CVE-2023-22523: This vulnerability can allow an attacker to perform privileged remote code execution on machines with the Assets Discovery agent installed.
- CVE-2023-22524: A remote code execution vulnerability that affects all versions of the Atlassian Companion App for MacOS, up to but not including Version 2.0.0.
- CVE-2022-1471: This vulnerability is a remote code execution flaw in the SnakeYAML library for Java.

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 Releases Security Advisories for Multiple Products
Atlassian Releases Security Advisories for Multiple Products | CISA

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

S2-066
S2-066 - Apache Struts 2 Wiki - Apache Software Foundation

SAP Security Patch Day – December 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

Microsoft December 2023 Patch Tuesday fixes 34 flaws, 1 zero-day
https://www.bleepingcomputer.com/news/microsoft/microsoft-december-2023-patch-tuesday-fixes-34-flaws-1-zero-day/

Microsoft December 2023 Patch Tuesday
https://isc.sans.edu/diary/Microsoft+Patch+Tuesday+December+2023/30480/

Microsoft Month Archives: December 2023
2023/12 | Microsoft Security Response Center

Mozilla Foundation Security Advisory 2023-56
Security Vulnerabilities fixed in Firefox 121 — Mozilla

Mozilla Foundation Security Advisory 2023-55
Security Vulnerabilities fixed in Thunderbird 115.6 — Mozilla

Mozilla Foundation Security Advisory 2023-54
Security Vulnerabilities fixed in Firefox ESR 115.6 — Mozilla

Mozilla Releases Security Updates for Firefox and Thunderbird
https://www.cisa.gov/news-events/alerts/2023/12/20/mozilla-releases-security-updates-firefox-and-thunderbird

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

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

Threat Actors Exploit Adobe ColdFusion CVE-2023-26360 for Initial Access to Government Servers

Threat Actors Exploit Adobe ColdFusion CVE-2023-26360 for Initial Access to Government Servers | 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