Office of
Information Security
Securing One HHS

Health Sector Cybersecurity
Coordination Center

HC3: Monthly Cybersecurity Vulnerability Bulletin
January 16, 2025 TLP:CLEAR Report: 202501161200

December Vulnerabilities of Interest to the Health Sector

In December 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 November are from Microsoft, Google/Android, Apple, Mozilla, Cisco, SAP, Adobe, Fortinet, Ivanti, VMware 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 fifteen (15) 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 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 seventy-four (74) CVEs. This month, there was one (1) zero-day vulnerability, which was reported to be actively exploited and addressed in the update, along with nineteen (19) Critical vulnerabilities that range in a CVSS score of 9.8 to 8.1. Microsoft has also reported on seven (7) non-Microsoft CVEs in their December release notes; all seven (7) impacted Chrome. This month's Patch Tuesday fixes one (1) zero-day, which has been actively exploited in attacks. The following one (1) actively exploited zero-day vulnerabilities is:

- CVE-2024-49138: Windows Common Log File System Driver Elevation of Privilege Vulnerability

HC3 encourages all users to follow CISA's guidance and apply any necessary updates, as a threat actor could exploit these vulnerabilities to take control of an affected system. For a complete list of Microsoft vulnerabilities and 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/Android released two updates in early December. The first update was released on December 01, 2024, and addressed six (6) vulnerabilities in the Framework, System, and there are no security issues addressed in Google Play system updates. All of these vulnerabilities were rated as high in severity, and according to Google: "The most severe of these issues could lead to local escalation of privilege with no additional execution privileges needed."

The second part of Google/Androids' security advisory was released on December 5th, 2024, and it addressed eight (8) vulnerabilities in the Kernel, Arm, Imagination Technologies, Unisoc, Qualcomm, and Qualcomm closed-source components. All eight (8) of these vulnerabilities were given a high rating in severity.

HC3 recommends 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. The Chrome browser update can be viewed here.

Apple

Apple released nine (9) security updates in December to address multiple vulnerabilities. HC3 encourages users and administrators to follow CISA's guidance and review the following advisories, applying necessary updates, as a threat actor could exploit these vulnerabilities to take control of an affected system:

- Safari 18.2
- visionOS 2.2
- iOS 18.2 and iPadOS 18.2
- macOS Ventura 13.7.2
- watchOS 11.2
- iPadOS 17.7.3
- tvOS 18.2
- macOS Sonoma 14.7.2
- macOS Sequoia 15.2

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 two (2) security advisories in December addressing vulnerabilities affecting Thunderbird: Zero (0) critical, seven (7) high, and one (1) moderate severity vulnerabilities. HC3 encourages all users to the following advisories and apply the necessary updates:

- **High**
  - Thunderbird 115.18
- **Moderate**
  - Thunderbird 128.5.2

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 (3) security updates to address vulnerabilities in multiple products. There were no critical rated updates release, one (1) update was rated as high impact, and the two (2) remaining updates were scored as having a medium impact. All three (3) had a CVSS score rating between 4.3 - 5.2 giving them all a medium severity rating.

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 ten (10) new security notes in December and three (3) 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. The new flaws consisted of one (1)“Critical”, two (2)“High”, five (5) “Medium” and two (2) “Low” rated vulnerabilities in severity. A breakdown of the one (1) Critical and two (2) highest rated High security notes for the month of December can be found below:

- **Security Note # 3536965:** (CVE-2024-47578) Multiple vulnerabilities in SAP NetWeaver AS for JAVA (Adobe Document Services). This vulnerability is rated CRITICAL and was given a CVSS score of 9.1. Product affected: SAP NetWeaver AS for JAVA (Adobe Document Services), Versions – ADSSSAP 7.50
- **Security Note # 3520281** (CVE-2024-47590): (Update to Security Note released on November 2024 Patch Day) This vulnerability was rated HIGH and was given a CVSS score of 8.8 and is a Cross-Site Scripting (XSS) vulnerability in SAP Web Dispatcher. Products affected: SAP Web Dispatcher, Versions – WEBDISP 7.77, 7.89, 7.93, KERNEL 7.77, 7.89, 7.93, 9.12, 9.13.
- **Security Note # 3469791** (CVE-2024-39592): Information Disclosure vulnerability through Remote Function Call (RFC) in SAP NetWeaver Application Server ABAP. This vulnerability was rated HIGH and was given a CVSS score of 8.5. Products affected: SAP NetWeaver Application Server ABAP, Version – KRNL64NUC 7.22, 7.22EXT, KRNL64UC 7.22, 7.22EXT, 7.53, KERNEL 7.22, 7.53, 7.54, 7.77, 7.89, 7.93.

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 customers visit the Support Portal and apply patches to protect their SAP landscape.

Adobe

Adobe released seventeen (17) security updates to address vulnerabilities for multiple different products. HC3 recommends all users follow CISA’s guidance and review the following bulletins, applying the necessary updates and patches immediately.

- APSB24-107 : Security update available for Adobe ColdFusion
- APSB24-69 : Security update available for Adobe Experience Manager
- APSB24-92 : Security update available for Adobe Acrobat and Reader
- APSB24-93 : Security update available for Adobe Media Encoder
- APSB24-94 : Security update available for Adobe Illustrator

- APSB24-95 : Security update available for Adobe After Effects
- APSB24-96 : Security update available for Adobe Animate
- APSB24-97 : Security update available for Adobe InDesign
- APSB24-98 : Security update available for Adobe PDFL SDK
- APSB24-99 : Security update available for Adobe Connect
- APSB24-100 : Security update available for Adobe Substance 3D Sampler
- APSB24-101 : Security update available for Adobe Photoshop
- APSB24-102 : Security update available for Adobe Substance 3D Modeler
- APSB24-103 : Security update available for Adobe Bridge
- APSB24-104 : Security update available for Adobe Premiere Pro
- APSB24-105 : Security update available for Adobe Substance 3D Painter
- APSB24-106 : Security update available for Adobe FrameMaker

HC3 recommends applying the appropriate security updates or patches that can be found on Adobe's Product Security Incident Response Team (PSIRT) by clicking here, as an attacker could exploit some of these vulnerabilities to control of a compromised system.

Fortinet

Fortinet's December vulnerability advisories addressed five (5) vulnerabilities. Zero (0) were rated critical, two (2) high, three (3) medium and zero (0) lows. HC3 recommends all users review Fortinet's Vulnerability Advisory page and apply all necessary updates and patches immediately.

VMware

VMware released zero (0) advisories. HC3 encourages all users to review the Broadcom Security Advisories - VMware Cloud Foundation page and follow CISA's guidance and apply any necessary updates.

Ivanti

Ivanti released Security Advisories for Ivanti Endpoint Manager, Ivanti Avalanche and Ivanti Connect Secure/Policy Secure, and five other Ivanti products totaling thirteen (13) vulnerabilities a threat actor could exploit to take control of and affected systems. HC3 encourages all users to review the Ivanti December Security Update page and follow CISA's guidance and apply any necessary updates:

Ivanti Cloud Service Application: Three (3) critical vulnerabilities
Ivanti Desktop and Server Management (DSM): One (1) High vulnerability
Ivanti Connect Secure and Policy Secure: Two (2) Critical and Three (3) High
Ivanti Sentry: One (1) High vulnerability
Ivanti Patch SDK: One (1) High vulnerability
Ivanti Application Control: One (1) High vulnerability
Ivanti Automation: One (1) High vulnerability
Ivanti Workspace Control: One (1) High vulnerability
Ivanti Performance Manager: One (1) High vulnerability
Ivanti Security Controls (iSec): One (1) High vulnerability

Atlassian

Atlassian released a security advisory regarding twelve (12) high-severity vulnerabilities in their December 2024 Security Bulletin. All of the vulnerabilities are rated between 8.1 to 7.1 on the CVSS scale. These vulnerabilities impact the Bitbucket Data Center and Server, Confluence Data Center and Server, and the Bamboo Data Center and Server. For a complete list of security advisories and bulletins from Atlassian, click here. HC3 recommends 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/docs/security/bulletin

Apple Security Releases
Apple security releases - Apple Support

Atlassian Security Bulletin
Security Advisories | Atlassian

Cisco Security Advisories
Security Advisories

Fortinet PSIRT Advisories
PSIRT Advisories | FortiGuard

Ivanti December Security Update
https://www.ivanti.com/blog/december-security-update

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

Microsoft December 2024 Security Updates
https://msrc.microsoft.com/update-guide/releaseNote/2024-Dec

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

SAP Security Patch Day – December 2024
https://support.sap.com/en/my-support/knowledge-base/security-notes-news/december-2024.html

VMware Security Advisories
https://support.broadcom.com/web/ecx/security-advisory?

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