# HC3: Monthly Cybersecurity Vulnerability Bulletin
# October 9, 2024 TLP:CLEAR Report: 202410091500

## September Vulnerabilities of Interest to the Health Sector

In September 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 September 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 19 vulnerabilities in September 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 87 vulnerabilities. There were four zero-day vulnerabilities, three of which are reported to be actively exploited, addressed in the update. Microsoft has also reported on 14 non-Microsoft CVEs that impact Chrome in their September release notes. Additional information on the zero-day vulnerabilities can be found below. 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.

- CVE-2024-38014: An attacker who successfully exploited this vulnerability could gain SYSTEM privileges.
- CVE-2024-38217: Windows Mark of the Web Security Feature Bypass Vulnerability
- CVE-2024-38226: Microsoft Publisher Security Feature Bypass Vulnerability
- CVE-2024-43491: A vulnerability in Servicing Stack has rolled back fixes for some previous vulnerabilities, which an attacker could exploit on Windows 10, version 1507.

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 September. The first update was released on September 01, 2024, and addressed ten vulnerabilities in the Framework, System, and 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/Android's security advisory was released on September 05, 2024, and it addressed updates in the Kernel, Arm, Imagination Technologies, Unisoc, Qualcomm, and Qualcomm closed-source components. Two of these vulnerabilities was rated as critical, and the remaining were given a high rating in severity. Additional information on the critical vulnerabilities from the National Vulnerability Database can be found below:

- CVE-2024-33042: Memory corruption when Alternative Frequency offset value is set to 255.
- CVE-2024-33052: Memory corruption when user provides data for FM HCI command control operations.

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 security updates in September to address multiple vulnerabilities. HC3 encourages users and administrators to follow CISA's guidance and review the following advisories, and apply necessary updates, as a threat actor could exploit these vulnerabilities to take control of an affected system:

- iOS 18 and iPadOS 18
- iOS 17.7 and iPadOS 17.7
- Safari 18
- macOS Sequoia 15
- macOS Sonoma 14.7
- macOS Ventura 13.7
- tvOS 18
- watchOS 11
- visionOS 2
- Xcode 16

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 seven security advisories in September addressing vulnerabilities affecting Thunderbird, Firefox for iOS, Firefox ESR, and Firefox. All these vulnerabilities were rated as high in severity. HC3 encourages all users to follow the below advisories and apply the necessary updates:

- Firefox for Android 130.0.1
- Thunderbird 115.15
- Thunderbird 128.2
- Focus for iOS 130
- Firefox ESR 115.15
- Firefox ESR 128.2
- Firefox 130

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 20 security updates to address vulnerabilities in multiple products. One of these updates was rated critical, ten were rated as high, and the remaining were scored as medium in severity. Additional information on the critical vulnerabilities can be found below:

- CVE-2024-20439, 20440: Multiple vulnerabilities in Cisco Smart Licensing Utility could allow an unauthenticated, remote attacker to collect sensitive information or administer Cisco Smart Licensing Utility services on a system while the software is running.

For a complete list of Cisco security advisories released in September, 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 16 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 was one reported vulnerability with a severity rating of "Hot News", which is the most severe and a top priority for SAP. The remaining flaws consisted of one "High", fourteen "Medium", and three "Low" rated vulnerabilities in severity. A breakdown of the High security notes can be found below:

- **Security Note #3479478** (CVE-2024-41730): This vulnerability was given a CVSS score of 9.8 and is a missing authorization check in SAP BusinessObjects Business Intelligence Platform.

For a complete list of SAP's security notes and updates for vulnerabilities released in September, 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 multiple security updates to address vulnerabilities for multiple different products. HC3 recommends all users follow CISA's guidance and review the following bulletins to apply the necessary updates and patches immediately.

- Security update available for Adobe Media Encoder | APSB24-53
- Security update available for Adobe Audition | APSB24-54
- Security update available for Adobe After Effects | APSB24-55
- Security update available for Adobe Premiere Pro | APSB24-58
- Security update available for Adobe Illustrator | APSB24-66
- Security update available for Adobe Acrobat Reader | APSB24-70
- Security update available for Adobe ColdFusion | APSB24-71
- Security update available for Adobe Photoshop | APSB24-72

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 these vulnerabilities to control a compromised system.

## Fortinet

Fortinet's September vulnerability advisories addressed two vulnerabilities. Both were rated as medium in severity and impact multiple products. The remaining vulnerability was rated as low in severity. If successful, a threat actor can exploit these vulnerabilities and take control of a compromised device or system. HC3 recommends all users review Fortinet's Vulnerability Advisory page, and apply all necessary updates and patches immediately:

- FG-IR-23-204
- FG-IR-24-051

## VMware

VMware released an advisory regarding vulnerabilities in the VMware Cloud Foundation and the vCenter Server. HC3 encourages all users to review the advisories and follow CISA's guidance to apply any necessary updates:

- VMSA-2024-001: VMware vCenter Server Updates

## Ivanti

Ivanti released three security updates for Ivanti Endpoint Manager, Ivanti Cloud Service Appliance, and Ivanti Workspace Control, which a threat actor could exploit to take control of and affected system. HC3 encourages all users to review the advisories and follow CISA's guidance to apply any necessary updates:

- Security Update for Cloud Services Appliance
- Security Updates for Endpoint Manager, Cloud Service Application, and Workspace Control

## Atlassian

Atlassian released a security advisory regarding 6 high-severity vulnerabilities in their September 2024 Security Bulletin. All of the vulnerabilities are rated as 7.5 on the CVSS scale and are tracked as CVE-2024-34750, CVE-2024-32007, CVE-2024-2985, CVE-2024-22871, and CVE-2024-29857. These vulnerabilities impact the Bamboo Data Center, Bitbucket Data Center, Confluence Data Center, and Crowd Data Center and are listed as a Denial of Service vulnerability. For a complete list of security advisories and bulletins from Atlassian can be viewed 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/security/bulletin

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

Atlassian Security Bulletin
Security Advisories | Atlassian

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

Fortinet PSIRT Advisories
PSIRT Advisories | FortiGuard

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

Microsoft September 2024 Patch Tuesday fixes 4 zero-days, 79 exploited flaws
https://www.bleepingcomputer.com/news/microsoft/microsoft-september-2024-patch-tuesday-fixes-4-zero-days-79-flaws/

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

Microsoft Month Archives: September 2024
2024/09 | Microsoft Security Response Center

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

SAP Security Patch Day – September 2024
SAP Security Patch Day – September 2024

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