# HC3: Monthly Cybersecurity Vulnerability Bulletin
# June 13, 2024 TLP:CLEAR Report: 202406131200

## May Vulnerabilities of Interest to the Health Sector

In May 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 May are from Baxter Welch Allyn, Microsoft, Google/Android, Apple, Mozilla, Cisco, SAP, 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 14 vulnerabilities in May 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.

### Baxter Welch Allyn

CISA released two ICS Medical Advisories for the Baxter Welch Allyn Connex Spot Monitor and Configuration Tool, and stated: "Successful exploitation of this vulnerability could allow an attacker to modify device configuration and firmware data/unintended exposure of credentials. Tampering with this data could lead to device compromise, resulting in impact and/or delay in patient care." Both vulnerabilities are remotely exploitable and are tracked as CVE-2024-1275 and CVE-2024-5176. Additional information on these vulnerabilities can be found below. HC3 is currently unaware of either of these vulnerabilities being exploited in the wild, but strongly encourages all users to apply any necessary updates or mitigations to prevent serious damage from occurring to the HPH sector:

- CVE-2024-5176 (CVSS v4 9.4): Insufficiently Protected Credentials vulnerability in

Baxter Welch Allyn Configuration Tool may allow Remote Services with Stolen Credentials. This issue affects Welch Allyn Configuration Tool: versions 1.9.4.1 and prior:

- CVE-2024-1275 (CVSS v4 9.1): Use of Default Cryptographic Key vulnerability in Baxter

Welch Ally Connex Spot Monitor may allow Configuration/Environment Manipulation. This issue affects Welch Ally Connex Spot Monitor in all versions prior to 1.52.

A new version of the product that mitigates the vulnerability will be available in Q3 2024, with no user action required for the update. Baxter recommends the following workarounds to help reduce risk:

- Apply proper network and physical security controls.
- Customers are advised to contact Baxter Technical Support or their Baxter Project Manager to create configuration files as needed. Baxter Technical Support can be reached at (800) 535-6663, option 2.

## Microsoft

Microsoft released or provided security updates for 60 vulnerabilities. There were two actively exploited zero-day vulnerabilities addressed in the update. One of these vulnerabilities was rated as critical in severity and is tracked as CVE-2024-30044, which is a flaw in SharePoint. Microsoft has also reported on 17 non-Microsoft CVEs in their May release notes, which impacts GitHub and Chrome. Additional information on the zero-day vulnerabilities from the national vulnerability database can be found below:

- CVE-2024-30040: Windows MSHTML Platform Security Feature Bypass Vulnerability
- CVE-2024-30051: Windows DWM Core Library Elevation of Privilege Vulnerability

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 May. The first update was released on May 01, 2024, and addressed eleven vulnerabilities in the Framework, System, and Google Play system. One of these vulnerabilities was given a critical rating, and the remaining were rated as high in severity. According to Google: "The most severe of these issues is a critical security vulnerability in the System component that could lead to local escalation of privilege with no additional execution privileges needed." The critical vulnerability is tracked as CVE-2024-23706 and impacts version 14 of Android. The second part of Google/Androids' security advisory was released on May 05, 2024, and it addressed updates in the Kernel, Kernel LTS Arm, MediaTek, Qualcomm components, and Qualcomm closed-source components. All vulnerabilities were rated as high. Additional information on the critical vulnerability can be found below:

- CVE-2024-23706: Possible bypass of health data permissions resulting from an improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed, and user interaction is not required.

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 multiple security updates in May, for several different products. HC3 recommends following CISA's guidance, which encourages users and administrators to review the following alerts and apply any

necessary updates:

- Safari 17.5
- iOS 17.5 and iPadOS 17.5
- iOS 16.7.8 and iPadOS 16.7.8
- macOS Sonoma 14.5
- macOS Ventura 13.6.7
- macOS Monterey 12.7.5
- watchOS 10.5
- tvOS 17.5

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 three security advisories in May addressing vulnerabilities affecting Firefox, Firefox ESR, Thunderbird, and Focus for iOS. All vulnerabilities were rated as high in severity. HC3 encourages all users to review the following advisories and apply the necessary updates:

- Firefox 126
- Firefox ESR 115.11
- Focus for iOS 126
- Thunderbird 115.11

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 19 security updates to address vulnerabilities in multiple products. Eight of the vulnerabilities were classified as "high" in severity, 1 as "informational". There were no critical vulnerabilities released from Cisco this month. Additionally, CISA released several security advisories on Cisco products, and reported that "a threat actor could exploit this vulnerability to take control of an affected system" along with a security publication impacting Cisco ASA, FMC, and FTD. HC3 encourages all users to review the following CISA advisories and apply the necessary updates:

- Cisco Crosswork Network Services Orchestrator
- Cisco Crosswork Network Services Orchestrator Privilege Escalation
- ConfD CLI Privilege Escalation and Arbitrary File Read and Write
- Cisco Secure Client for Windows with Network Access Manager Module Privilege Escalation
- Cisco Crosswork Network Services Orchestrator Open Redirect
- Cisco Secure Email and Web Manager, Secure Email Gateway and Secure Web Vulnerabilities
- Cisco Secure Email Gateway HTTP Response Splitting
- Cisco AppDynamics Network Visibility Service Denial of Service

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

# HC3: Monthly Cybersecurity Vulnerability Bulletin
# June 13, 2024 TLP:CLEAR Report: 202406131200

## SAP

SAP released 14 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 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 one "High", ten "Medium", and three "Low" rated vulnerabilities in severity. A breakdown of the Hot News security notes for the month of May can be found below:

- **Security Note #2622660** (No associated CVE): This is an update to the security note released on April 2018 for the browser control Google Chromium delivered with SAP Business Client.
- **Security Note #3455438** (CVE-2019-17495): This vulnerability was given a CVSS score of 9.8; relates with multiple vulnerabilities in SAP CX Commerce.
- **Security Note #3448171** (CVE-2024-33006): This vulnerability was given a CVSS score of 9.6 and it is a file upload vulnerability in SAP NetWeaver Application Server ABAP and ABAP Platform, impacting multiple versions.

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

- Adobe Acrobat and Reader
- Adobe Illustrator
- Substance 3D Painter
- Adobe Aero
- Substance 3D Designer
- Adobe Animate
- Adobe FrameMaker
- Adobe Dreamweaver

## Fortinet

Fortinet's May vulnerability advisories addressed five vulnerabilities. All vulnerabilities were rated as medium in severity. The highest of these vulnerabilities is rated with a CVSSv3 score 6.8 and is tracked as CVE-2023-46714, and can result in the execution of a stack-based buffer overflow [CWE-121] vulnerability in FortiOS administrative interface. This vulnerability may allow an attacker to execute arbitrary code or commands via crafted HTTP or HTTPs requests. If successful, a threat actor can exploit this vulnerability 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-23-415
- FG-IR-23-195
- FG-IR-24-017
- FG-IR-23-225
- FG-IR-23-137

## Atlassian

Atlassian released a security advisory regarding 35 high-severity vulnerabilities and 2 critical-severity

vulnerabilities in their May 2024 Security Bulletin. Both of the critical vulnerabilities were rated as 9.8 on the CVSS scale and both are associated with CVE-2024-1597, which can allow an attacker to inject SQL queries on a vulnerable system. Atlassian stated in their bulletin that "Jira Software Data Center and Confluence Data Center is unaffected by this vulnerability, as they do not use the PreferQueryMode=SIMPLE in their SQL database connection settings. Whilst the default configuration is safe, the vulnerability remains in the driver that ships with Confluence/Jira Data Center."

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/security/bulletin

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

Atlassian Security Bulletin
Security Advisories | Atlassian

Baxter Welch Allyn Connex Spot Monitor
https://www.cisa.gov/news-events/ics-medical-advisories/icsma-24-151-02

Baxter Welch Allyn Configuration Tool
https://www.cisa.gov/news-events/ics-medical-advisories/icsma-24-151-01

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

Fortinet PSIRT Advisories
PSIRT Advisories | FortiGuard

Microsoft May 2024 Patch Tuesday fixes 3 zero-days, 61 flaws
https://www.bleepingcomputer.com/news/microsoft/microsoft-may-2024-patch-tuesday-fixes-3-zero-days-61-flaws/

Microsoft May 2024 Patch Tuesday
https://msrc.microsoft.com/update-guide/releaseNote/2024-May

Microsoft Month Archives: May 2024
2024/05 | Microsoft Security Response Center

Mozilla Foundation Security Advisory 2024-21
Security Vulnerabilities fixed in Firefox 126 — Mozilla

Mozilla Foundation Security Advisory 2024-22
Security Vulnerabilities fixed in Firefox ESR 115.11 — Mozilla

Mozilla Foundation Security Advisory 2024-23
Security Vulnerabilities fixed in Thunderbird 115.11 — Mozilla

Mozilla Foundation Security Advisory 2024-14
Security Vulnerabilities fixed in Focus for iOS 126 — Mozilla

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 – May 2024
SAP Security Patch Day – May 2024

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