HC3: Monthly Cybersecurity Vulnerability Bulletin
November 7, 2024 TLP:CLEAR Report: 202411071500

October Vulnerabilities of Interest to the Health Sector

In October 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 October 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 given 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 17 vulnerabilities in October 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 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 130 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 19 non-Microsoft CVEs in their October release notes that impact Chrome. 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-2024-43573: Windows MSHTML Platform Spoofing Vulnerability
- CVE-2024-43572: Microsoft Management Console Remote Code Execution Vulnerability
- CVE-2024-20659: Windows Hyper-V Security Feature Bypass Vulnerability
- CVE-2024-43583: Winlogon Elevation of Privilege Vulnerability
- CVE-2024-6197: Open-Source Curl Remote Code Execution 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 October. The first update was released on October 01, 2024, and addressed nine vulnerabilities in the Framework, System, and Google Play system updates. All 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 October 05, 2024, and it addressed 19 vulnerabilities in the Kernel, Arm, Imagination Technologies, Unisoc, Qualcomm, and Qualcomm closed-source components. None of these vulnerabilities was rated as critical, and all were given a high rating in severity.

HC3 recommends users refer to the Android and Google service mitigations web page 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.

Apple

Apple released 11 security updates in October 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 18.0.1 and iPadOS 18.0.1
- Apple TV 1.5.0.152 for Windows
- visionOS 2.1
- tvOS 18.1
- watchOS 11.1
- macOS Ventura 13.7.1
- macOS Sonoma 14.7.1
- macOS Sequoia 15.1
- iOS 17.7.1 and iPadOS 17.7.1
- iOS 18.1 and iPadOS 18.1
- Safari 18.1

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 15 security advisories in October addressing vulnerabilities affecting Thunderbird, Firefox for iOS, Firefox ESR, and Firefox—two critical, 11 high, and two moderate in severity vulnerabilities. HC3 encourages all users to review the following advisories and apply the necessary updates:

- Critical
  - Thunderbird 131.0.1, Thunderbird 128.3.1, Thunderbird 115.16.0
  - Firefox 131.0.2, Firefox ESR 128.3.1, Firefox ESR 115.16.1
- High
  - Thunderbird 132
  - Thunderbird 128.4
  - Firefox ESR 115.17
  - Firefox ESR 128.4
  - Firefox ESR 128.3
  - Firefox 131

- Firefox 131.0.3
- Firefox 132
- Thunderbird 131
- Thunderbird 128.3
- Firefox ESR 115.16

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 54 security updates to address vulnerabilities in multiple products. Four of these updates were rated critical, 16 were rated as high, and the remaining were scored as medium in severity.

Additional information on the critical vulnerabilities can be found below:

- CVE-2024-20412: A vulnerability in Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 1000, 2100, 3100, and 4200 Series could allow an unauthenticated, local attacker to access an affected system using static credentials. This vulnerability is due to the presence of static accounts.
- CVE-2024-20424: A vulnerability in the web-based management interface of Cisco Secure Firewall Management Center (FMC) Software, formerly Firepower Management Center Software, could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system.
- CVE-2024-20329: This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by submitting crafted input when executing remote CLI commands over SSH. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system.
- CVE-2024-20432: This vulnerability is due to improper user authorization and insufficient validation of command arguments. An attacker could exploit this vulnerability by submitting crafted commands to an affected REST API endpoint, or through the web UI. A successful exploit could allow the attacker to execute arbitrary commands on the CLI of a Cisco NDFC-managed device with network-admin privileges.

For a complete list of Cisco security advisories released in October, 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 13 security notes in October and seven 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. Flaws consisted of one "Critical", three "High", and nine "Medium" rated vulnerabilities in severity. A breakdown of the High security notes for the month of October can be found below:

- **Security Note # 3479478** (CVE-2024-41730): This vulnerability was given a CVSS score of 9.8 and is a Missing Authentication check in SAP BusinessObjects Business Intelligence Platform. If Single Signed On is enabled on Enterprise authentication, an unauthorized user can get a logon token using a REST

endpoint. The attacker can fully compromise the system, resulting in High impact on confidentiality, integrity, and availability.

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

- APSB24-52 : Security update available for Adobe Substance 3D Painter
- APSB24-73 : Security update available for Adobe Commerce
- APSB24-74 : Security update available for Adobe Dimension
- APSB24-76 : Security update available for Adobe Animate
- APSB24-82 : Security update available for Adobe FrameMaker
- APSB24-78 : Security update available for Adobe Lightroom
- APSB24-79 : Security update available for Adobe InCopy
- APSB24-80 : Security update available for Adobe InDesign
- APSB24-81 : Security update available for Adobe Substance 3D Stager

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

Fortinet

Fortinet's October vulnerability advisories addressed six vulnerabilities. Two were rated critical, one rated high, one rated medium, and two rated low. The critical vulnerabilities impact multiple products. 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. The critical vulnerabilities are:

- FG-IR-24-423 (CVE-2024-47575) Missing authentication in fgfmsd
- FG-IR-24-029 (CVE-2024-23113) Format String Bug in fgfmd

VMware

VMware released one high-rated advisory regarding authenticated SQL injection vulnerability in VMware HCX. HC3 encourages all users to review the below advisories and follow CISA's guidance to apply any necessary updates:

- VMSA-2024-0021 (CVE-2024-38814): Authenticated SQL injection vulnerability

Ivanti

Ivanti released Security Advisories for Ivanti Endpoint Manager, Ivanti Cloud Service Appliance, Ivanti Velocity License Server, Ivanti Avalanche, and Ivanti Connect Secure/Policy Secure, totaling 11 vulnerabilities a threat actor could exploit to take control of and affected system. HC3 encourages all users to review the below advisories and follow CISA's guidance to apply any necessary updates:

- Ivanti Endpoint Manager Mobile (EPMM)
  Ivanti CSA (Cloud Services Application)
- Velocity License Server (CVE-2024-9167)
- Ivanti Avalanche 6.4.5 (Multiple CVE's)
- Ivanti Connect Secure and Policy Secure

Atlassian

Atlassian released a security advisory regarding 6 high-severity vulnerabilities in their October 2024 Security Bulletin. All of the vulnerabilities are rated between 7.3 to 8.1 on the CVSS scale and are tracked as CVE-2024-21147, CVE-2024-4367, CVE-2022-31129, CVE-2022-24785, CVE-2024-29131 and CVE-2024-7254. These vulnerabilities impact the Bitbucket Data Center and Server, Confluence Data Center and Server, and Jira Service Management 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 October Security Update
https://www.ivanti.com/blog/october-2024-security-update

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

Microsoft October 2024 Security Updates
October 2024 Security Updates - Release Notes - Security Update Guide - Microsoft

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

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