HC3: Monthly Cybersecurity Vulnerability Bulletin
December 9, 2024 TLP:CLEAR Report: 202412091700

November Vulnerabilities of Interest to the Health Sector

In November 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 twenty-two (22) vulnerabilities in November 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 89 CVEs. There were four zero-day vulnerabilities, three of which are reported to be actively exploited, addressed in the update. Microsoft has also reported on three (3) non-Microsoft CVEs in their November release notes: two (2) impacted Chrome, and one (1) OpenSSL. This month's Patch Tuesday fixes four zero-days, two of which were actively exploited in attacks, and two (2) others publicly disclosed. Additional information on the zero-day vulnerabilities can be found below. The following two (2) actively exploited zero-day vulnerabilities are:

- CVE-2024-43451: NTLM Hash Disclosure Spoofing Vulnerability
- CVE-2024-49039: Windows Task Scheduler Elevation of Privilege Vulnerability

The following two (2) vulnerabilities were publicly disclosed but not actively exploited:

- CVE-2024-49040: Microsoft Exchange Server Spoofing Vulnerability
- CVE-2024-49019: Active Directory Certificate Services 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 November. The first update was released on November 1, 2024, and addressed twenty-one (21) vulnerabilities in the Framework, System, and Google Play system updates. All 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 November 5, 2024, and it addressed twenty-five (25) vulnerabilities in the Kernel, Arm, Imagination Technologies, Unisoc, Qualcomm, and Qualcomm closed-source components. Twenty-four (24) of these vulnerabilities were given a high rating in severity. One (1) a Qualcomm closed-source components was given a Critical severity rating:

- CVE-2024-38408: Cryptographic issue when a controller receives an LMP start encryption command under unexpected conditions.

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 five (5) security updates in November to address multiple vulnerabilities. HC3 encourages users and administrators to follow CISA's guidance and review the following advisories, along with applying necessary updates, as a threat actor could exploit these vulnerabilities to take control of an affected system:

- Safari 18.1.1
- visionOS 2.1.1
- iOS 18.1.1 and iPadOS 18.1.1
- iOS 17.7.2 and iPadOS 17.7
- macOS Sequoia 15.1.1

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 eight (8) security advisories in November addressing vulnerabilities affecting Thunderbird, Firefox for iOS, Firefox ESR, and Firefox: zero (0) critical, seven (7) high and one (1) moderate severity vulnerabilities. HC3 encourages all users to follow the advisories and apply the necessary updates:

- High
  - Thunderbird 128.5
  - Thunderbird 133
  - Firefox ESR 115.18
  - Thunderbird 128.4.3

- Firefox ESR 128.5
- Firefox 133
- Thunderbird 132.0.1

A complete list of Mozilla's updates, including lower severity vulnerabilities, is 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 seventeen (17) security updates to address vulnerabilities in multiple products. One (1) of these updates were rated critical, three (3) were rated as high, and the remaining were scored as medium in severity. Additional information on the critical vulnerabilities can be found below:

- CVE-2024-20418: A vulnerability in the web-based management interface of Cisco Unified Industrial Wireless Software for Cisco Ultra-Reliable Wireless Backhaul (URWB) Access Points could allow an unauthenticated, remote attacker to perform command injection attacks with root privileges on the underlying operating system. This vulnerability is due to improper validation of input to the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system of the affected device.

For a complete list of Cisco security advisories released in November, 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 eight (8) new security notes in November and two (2) 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 zero (0)"Critical", two (2)"High", six (6) "Medium" and two (2) "Low" rated vulnerabilities in severity. A breakdown of the High security notes for the month of November can be found below:

- Security Note # 3520281 (CVE-2024-47590): This vulnerability was given a CVSS score of 8.8 and is a Cross-Site Scripting (XSS) vulnerability in SAP Web Dispatcher. Product: SAP Web Dispatcher, Versions – WEBDISP 7.77, 7.89, 7.93, KERNEL 7.77, 7.89, 7.93, 9.12, 9.13
- Security Note # 3483344 (CVE-2024-39592): This vulnerability was given a CVSS score of 7.7 and Missing Authorization check in SAP PDCE. Product: SAP PDCE, Version – S4CORE 102, 103, S4COREOP 104, 105, 106, 107, 108.

For a complete list of SAP's security notes and updates for vulnerabilities released in November, 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.

HC3: Monthly Cybersecurity Vulnerability Bulletin
December 9, 2024 TLP:CLEAR Report: 202412091700

Adobe

Adobe released nine (9) 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.

- APSB24-77 : Security update available for Adobe Bridge
- APSB24-85 : Security update available for Adobe After Effects
- APSB24-87 : Security update available for Adobe Illustrator
- APSB24-88 : Security update available for Adobe InDesign
- APSB24-90 : Security update available for Adobe Commerce
- APSB24-83 : Security update available for Adobe Audition
- APSB24-86 : Security update available for Adobe Substance 3D Painter
- APSB24-89 : Security update available for Adobe Photoshop
- APSB24-91 : Security update available for Adobe InDesign

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 November vulnerability advisories addressed fifteen (15) vulnerabilities. One (1) was rated critical, three (3) high, seven (7) medium and four (4) 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 vulnerability is:

- FG-IR-24-423 Missing authentication in fgfmsd: CVE-2024-47575

VMware

VMware released one (1) high advisory regarding VMware Aria Operations containing a local privilege escalation vulnerability. VMware has evaluated the severity of this issue to be in the range with a maximum CVSSv3 base score of 7.8. VMware Aria Operations updates address multiple vulnerabilities. HC3 encourages all users to review the Broadcom Security Advisories - VMware Cloud Foundation page and follow CISA's guidance and apply any necessary updates:

- VMSA-2024-0022 (CVE-2024-38830): Local privilege escalation vulnerability

Ivanti

Ivanti released Security Advisories for Ivanti Endpoint Manager, Ivanti Avalanche and Ivanti Connect Secure/Policy Secure, totaling fifty-nine (59) vulnerabilities that a threat actor could exploit to take control of affected systems. HC3 encourages all users to review the Ivanti November Security Update page and follow CISA's guidance and apply any necessary updates:

- Ivanti EPM
- Ivanti Avalanche
- Ivanti Connect Secure, Ivanti Policy Secure and Ivanti Security Access Client

Atlassian

Atlassian released a security advisory regarding nineteen (19) high-severity vulnerabilities in their November 2024 Security Bulletin. All of the vulnerabilities are rated between 7.5 to 8.8 on the CVSS scale. These vulnerabilities impact the Bitbucket Data Center and Server, Confluence Data Center and Server, Jira Service Management Data Center and Server, Jira Data Center and Server, Bamboo Data Center and Server, Crowd Data Center and Server, Sourcetree for Mac, and Sourcetree for Windows. 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 November Security Update
https://www.ivanti.com/blog/november-2024-security-update

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

Microsoft November 2024 Security Updates
https://msrc.microsoft.com/update-guide/releaseNote/2024-Nov

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

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