HC3: Monthly Cybersecurity Vulnerability Bulletin
December 4, 2023 TLP:CLEAR Report: 202312041200

November Vulnerabilities of Interest to the Health Sector

In November 2023, 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, VMWare, Adobe, Fortinet, Atlassian, Becton, Dickinson (BD) and Company, and ownCloud. 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 18 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 that 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 63 vulnerabilities, including five zero-days. Three of these vulnerabilities were list as critical, 56 were rated as important, and the remaining four were rated as moderate in severity. The highest of these vulnerabilities were given a base score of 9.8 and are tracked as CVE-2023-36028 and CVE-2023-36397. CVE-2023-36028 can allow an unauthenticated attacker to exploit a Microsoft Protected Extensible Authentication Protocol (PEAP) Server by sending malicious PEAP packets over the network. CVE-2023-36397 can be exploited when the Windows message queuing service is running in a PGM Server environment, and an attacker could send a crafted file to achieve remote code execution. Additional information on the zero-day exploits can be found below:

- CVE-2023-36025 (CVSS score: 8.8) - Windows SmartScreen Security Feature Bypass Vulnerability
- CVE-2023-36033 (CVSS score: 7.8) - Windows DWM Core Library Elevation of Privilege Vulnerability
- CVE-2023-36036 (CVSS score: 7.8) - Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
- CVE-2023-36038 (CVSS score: 8.2) - ASP.NET Core Denial of Service Vulnerability
- CVE-2023-36413 (CVSS score: 6.5) - Microsoft Office Security Feature Bypass Vulnerability

For a complete list of Microsoft vulnerabilities and security updates, click here. HC3 recommends that 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 early in November which addressed 37 vulnerabilities. According to Google: "The most severe of these issues is a critical security vulnerability in the System component that could lead to local information disclosure with no additional execution privileges needed." The vulnerability is tracked as CVE-2023-40113 and impacts versions 11, 12, 12L, 13 of Android. The remaining vulnerabilities were given a high severity rating. The second part of Google/Androids's November security advisory addressed 22 updates in the Arm, MediaTek, and Qualcomm components.

Towards the end of November, Google Chrome released an update to fix seven flaws with one of the vulnerabilities being actively exploited. The vulnerability that was exploited in the wild is tracked as CVE-2023-6345. CVE-2023-6345 is an integer overflow in Skia, in Google Chrome, prior to version 119.0.6045.199, and this can allow for a remote attacker who has compromised the renderer process to perform a sandbox escape through a malicious file. A complete list of details for the seven vulnerabilities can be accessed here.

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 should follow previous guidance to prevent their devices from being compromised. All Android and Google service mitigations, along with security information on vulnerabilities for the month of November, can be viewed by clicking here, and the Chrome browser update can be viewed here.

Apple

Apple released four security updates on November 7, 2023, for several different products. None of these security updates were associated with any published CVEs. The impacted devices are listed below:

- iOS 17.1.1 and iPadOS 17.1.1
- macOS Ventura 13.6.2
- macOS Sonoma 14.1.1
- watchOS 10.1.1

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 security advisories in November addressing vulnerabilities affecting multiple Mozilla products, including Firefox iOS 120, Firefox 120, Firefox ESR, and Thunderbird. If successful, a threat actor could exploit these vulnerabilities to take control of a compromised system or device. HC3 encourages all users to follow CISA's guidance to review the following advisories and apply the necessary updates:

- Firefox iOS 120
- Firefox 120
- Firefox ESR 115.5
- Firefox Thunderbird 115.5

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 36 security updates to address vulnerabilities in multiple products. Three were classified as "Critical" in severity, 11 as "High," and the remaining were classified as "Medium" in severity. The three critical vulnerabilities impact the Cisco Firepower Management Software (CVE-2023-20048) and multiple vulnerabilities were identified within the Cisco IOS XE Software (CVE-2023-20198, CVE-2023-20273), along with the DHCP relay subsystem for Cisco IOS and IOS XE software (CVE-2017-12240). If successful, a cyber threat actor can exploit some of these vulnerabilities to execute unauthorized configuration commands or conduct remote code execution. Additionally, a joint cybersecurity advisory was released highlighting the active exploiting of CVE-2023-4966 (which has been referred to as Citrix Bleed) from LockBit 3.0. CVE-2023-4966 is a buffer overflow vulnerability that exists within the Citrix NetScaler ADC and NetScaler appliances. The exploitation of this vulnerability can allow a threat actor to bypass multi-factor authentication (MFA) and hijack legitimate user sessions. HC3 recommends following CISA's guidance, which strongly urges users and administrators to review the following advisories and apply updates immediately:

- Cisco Firepower Management Center Software Command Injection Vulnerability
- Cisco Identity Services Engine Command Injection Vulnerabilities
- Cisco Identity Services Engine Vulnerabilities
- Cisco Firepower Threat Defense Software for Cisco Firepower 2100 Series Firewalls Inspection Rules Denial of Service Vulnerability
- Cisco Firepower Threat Defense Software ICMPv6 with Snort 2 Denial of Service Vulnerability
- Cisco Firepower Threat Defense Software and Firepower Management Center Software Code Injection Vulnerability
- Cisco Firepower Management Center Software Log API Denial of Service Vulnerability
- Cisco Firepower Management Center Software Command Injection Vulnerabilities
- Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Remote Access VPN Denial of Service Vulnerability
- Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software ICMPv6 Message Processing Denial of Service Vulnerability

It should also be noted that the manufacturer has warned that these compromised sessions for the Citrix Bleed vulnerability will still be active after a patch has been implemented. HC3 encourages all administrators to follow Citrix's guidance to upgrade their devices and remove any active or persistent sessions with the following commands:

- kill aaa session -all

- kill icaconnection -all
- kill rdp connection -all
- kill pcoipConnection -all
- clear lb persistentSessions

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 three new 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 new vulnerability with a severity rating of "Hot News," which is the most severe and a top priority for SAP. The remaining flaws were rated as "Medium" in severity. A breakdown of the new security notes for the month of November can be found below:

- **Security Note #3355658** (CVE-2023-31403)**:** This vulnerability was given a CVSS score of 9.6 and it is an Improper Access Control vulnerability in SAP Business One product installation, version 10.0.
- **Security Note #3362849** (CVE-2023-41366)**:** This vulnerability was given a CVSS score of 5.3 and it is an information disclosure vulnerability in the SAP NetWeaver Application Server ABAP and ABAP platform, and impacts multiple versions.
- **Security Note #3366410** (CVE-2023-42480)**:** This vulnerability was given a CVSS score of 5.3 and it is an information disclosure vulnerability in NetWeaver AS Java Logon in version 7.50.

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.

VMWare

VMWare released one critical security advisory update regarding an authentication bypass vulnerability in the VMware Cloud Director Appliance. A remote attacker could exploit some of these vulnerabilities to take control of an affected system. Additional information on the critical vulnerability is listed below:

- VMSA-2023-0026 (CVE-2023-34060) was rated as critical in severity and was assigned a CVSSv3 score of 9.8. Through this vulnerability, a malicious actor with network access to the appliance can bypass login restrictions through port 22 (SSH) and port 5480 (appliance management console) in the VMware Cloud Director appliance once it is upgraded to version 10.5.

For a complete list of VMWare's security advisories, click here. Patches are available to remediate these vulnerabilities found in VMWare products. To remediate the listed vulnerabilities, apply the updates listed in the 'Fixed Version' column of the 'Response Matrix' below to affected deployments. HC3 recommends that users follow VMWare's guidance for each and apply patches listed in the 'Fixed Version' column of the

'Response Matrix' that can be accessed by clicking directly on the security advisory.

Adobe

Adobe released security advisories to address multiple critical and important vulnerabilities in Adobe software. If successful, a threat actor could exploit some of these vulnerabilities to escalate their privileges or conduct arbitrary code execution. HC3 recommends that all users review the Adobe Security Bulletins and follow CISA's guidance, which encourages users and administrators to review the following advisories and apply the necessary updates:

- Adobe ColdFusion
- Adobe RoboHelp Server
- Adobe Acrobat and Reader
- Adobe InDesign
- Adobe Photoshop
- Adobe Bridge
- Adobe FrameMaker Publishing Server
- Adobe InCopy
- Adobe Animate
- Adobe Dimension
- Adobe Media Encoder
- Adobe Audition
- Adobe Premiere Pro
- Adobe After Effects

For a complete list of Adobe security updates, click here. HC3 recommends that all users apply necessary updates and patches immediately

Fortinet

Fortinet's November vulnerability advisory addressed several vulnerabilities across different Fortinet products. Two of the advisories came with a high rating in severity and one classified as medium in severity. The highest was rated with a CVSS score of 7.4 and is tracked as CVE-2023-41840 and can result in the escalation of privileges in the FortiClient Windows OpenSSL component. If successful, a threat actor can exploit this vulnerability and take control of a compromised device or system. HC3 recommends that all users review Fortinet's Vulnerability Advisory page and apply all necessary updates and patches immediately:

- FG-IR-22-299
- FG-IR-23-385
- FG-IR-23-274

Atlassian

Atlassian released a security advisory regarding 26 high-severity vulnerabilities in their November 2023 Security Bulletin. All the vulnerabilities were rated as "high" in severity, and the highest was given a CVSS score of 8.5, which is tracked as CVE-2023-22516. CVE-2023-22516 is a remote code execution vulnerability in the Bamboo Data Center and Server. Additionally, in an advisory from CISA, CVE-2023-22518 was highlighted in early November as a flaw that could be exploited in the Confluence Data Center, and that a threat actor could use this vulnerability to obtain sensitive data. Further investigation of this revealed active exploiting and ransomware being deployed through CVE-2023-22518. The full advisory can be viewed here. HC3 strongly encourages users and administrators to view the advisory and to apply upgrades provided by Atlassian. A complete list of security advisories and bulletins from Atlassian can be viewed here.

Becton, Dickinson and Company

Becton, Dickinson and Company announced several vulnerabilities in the FACSChorus software that were also identified in an ICS Medical Advisory, from CISA, on November 28, 2023. The vulnerabilities range from low to medium in severity, but successful exploitation of these vulnerabilities can result in a threat actor gaining the ability to change system configurations, obtain access to sensitive information, or system components. Additional information on the top three highest-rated vulnerabilities can be found below, and the complete advisory and vulnerability details from Becton, Dickinson and Company can be viewed here.

- CVE-2023-29060 – Lack of USB Whitelisting (CVSS 5.4): In this vulnerability, the FACSChorus workstation operating system does not restrict what devices can interact with its USB ports. This could allow a threat actor with physical access to the workstation to gain access to system information and exfiltrate data.
- CVE-2023-29061 – Lack of Adequate BIOS Authentication (CVSS 5.2): A threat actor with physical access to the workstation can access the BIOS configuration and modify the drive boot order and BIOS pre-boot authentication.
- CVE-2023-29064 – Hardcoded Secrets (CVSS 4.1): In this vulnerability, the FACSChorus software contains sensitive information, which is stored in plaintext. A threat actor could obtain this information in the application, which could include tokens and passwords for administrative-level accounts.

ownCloud

ownCloud announced a critical vulnerability that was given a 10 out of 10 in severity on the CVSS scale. The vulnerability is tracked as CVE-2023-49103, which impacts the "graphapi" app in ownCloud and can allow for a threat actor to obtain administrative passwords, mail server credentials, and license keys. According to a report from GreyNoise, this vulnerability is being widely exploited in the wild since November 25, 2023.

Additional information on CVE-2023-49103, along with mitigations from the manufacturer, can be viewed here. HC3 strongly encourages all uses to follow the vendor's instructions in the "Action Taken" section of the alert.

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

BD FACSChorus Vulnerabilities - Software and Workstation
https://www.bd.com/en-us/about-bd/cybersecurity/bulletin/bd-facschorus-software

BD FACSChorus
https://www.cisa.gov/news-events/ics-medical-advisories/icsma-23-331-01

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

CVE-2023-49103: ownCloud Critical Vulnerability Quickly Exploited in the Wild
https://www.greynoise.io/blog/cve-2023-49103-owncloud-critical-vulnerability-quickly-exploited-in-the-wild

Disclosure of sensitive credentials and configuration in containerized deployments
https://owncloud.com/security-advisories/disclosure-of-sensitive-credentials-and-configuration-in-containerized-deployments/

VMware Releases Security Update for Cloud Director Appliance
VMware Releases Security Update for Cloud Director Appliance | CISA

VMware Security Advisories
https://www.vmware.com/security/advisories.html

Fortinet PSIRT Advisories
PSIRT Advisories | FortiGuard

SAP Security Patch Day – November 2023
https://dam.sap.com/mac/app/e/pdf/preview/embed/ucQrx6G?ltr=a&rc=10

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

Microsoft November 2023 Patch Tuesday fixes 5 zero-days, 58 flaws
https://www.bleepingcomputer.com/news/microsoft/microsoft-november-2023-patch-tuesday-fixes-5-zero-days-58-flaws/

Microsoft November 2023 Patch Tuesday
https://isc.sans.edu/diary/Microsoft+Patch+Tuesday+November+2023/30400

Microsoft Month Archives: November 2023
https://msrc.microsoft.com/blog/2023/11/

Mozilla Foundation Security Advisory 2023-52
https://www.mozilla.org/en-US/security/advisories/mfsa2023-52/

Mozilla Foundation Security Advisory 2023-51
https://www.mozilla.org/en-US/security/advisories/mfsa2023-51/

Mozilla Foundation Security Advisory 2023-50
https://www.mozilla.org/en-US/security/advisories/mfsa2023-50/

Mozilla Foundation Security Advisory 2023-49
https://www.mozilla.org/en-US/security/advisories/mfsa2023-49/

Mozilla Releases Security Updates for Firefox and Thunderbird
https://www.cisa.gov/news-events/alerts/2023/11/22/mozilla-releases-security-updates-firefox-and-thunderbird

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

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

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