HC3: Monthly Cybersecurity Vulnerability Bulletin
November 03, 2023 TLP:CLEAR Report: 202311031200

October Vulnerabilities of Interest to the Health Sector

In October 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 October are from Microsoft, Google/Android, Apple, Mozilla, Cisco, SAP, VMWare, Adobe, Fortinet, Atlassian, SolarWinds, NextGen Healthcare, and F5. A vulnerability is given the classification as 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. The sections that follow are of 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 eighteen 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 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 103 vulnerabilities, including three zero-days. Thirteen of these vulnerabilities were listed as critical and were remote code execution flaws, with the highest two (base score 9.8) tracked as CVE-2023-35349, which is a Microsoft Message Queuing RCE vulnerability, and CVE-2023-36434, which can lead to an elevation of privileges in Windows IIS. The remaining vulnerabilities were tagged as important. All three of the zero-day vulnerabilities were observed being actively exploited by threat actors. Additional information on these exploits can be found below:

- CVE-2023-44487: (CVSS 7.5) This vulnerability has also been referred to as Rapid Reset, which is a vulnerability that can allow a malicious actor to conduct a DDoS attack against the HTTP/2 protocol. Through this, an attacker could bring down a server by exhausting all of its resources.
- CVE-2023-36563: (CVSS 6.5) An information disclosure vulnerability in Microsoft WordPad, through NTLM hashes.
- CVE-2023-41763: (CVSS 5.3) This a vulnerability that can allow for an elevation of privileges through Microsoft Skype for Business. According to Microsoft: "An attacker could make a specially crafted network call to the target Skype for Business server, which could cause the parsing of an http request made to an arbitrary address. This could disclose IP addresses, or port numbers, or both to the attacker."

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.

HC3: Monthly Cybersecurity Vulnerability Bulletin
November 03, 2023 TLP:CLEAR Report: 202311031200

Google/Android

Google/Android released two updates early in October which addressed 51 vulnerabilities, including two zero-days, with one given a high severity rating and the other a medium severity rating. Both have been potentially exploited in the wild. These zero-days are tracked as CVE-2023-4863 (CVSS 8.8) and CVE-2023-4211 (CVSS 5.5). CVE-2023-4863 is a remote code execution vulnerability that can allow a heap buffer overflow in libwebp in Google Chrome prior to 116.0.5845.187 and libwebp 1.3.2, allowing a remote attacker to perform an out-of-bounds memory write through a crafted HTML page. CVE-2023-4211 can allow for a local non-privileged user to make GPU memory processing operations to obtain access to already freed memory. According to a Google advisory: "There are indications that CVE-2023-4863 and CVE-2023-4211 may be under limited, targeted exploitation." Of the 51 flaws fixed, five of these were rated as critical. CVE-2023-40129 and the previously mentioned CVE-2023-4863 are both remote code execution vulnerabilities. CVE-2023-24855, CVE-2023-28540, and CVE-2023-33028 are vulnerabilities that affected Qualcomm closed-sourced components, and are further addressed in the Qualcomm October 2023 Security Bulletin. The remaining vulnerabilities were given a high severity rating.

HC3 recommends that 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. All Android and Google service mitigations, along with security information on vulnerabilities, can be viewed by clicking here, and the Chrome browser update can be viewed here.

Apple

Apple released multiple security updates to address vulnerabilities in different products, along with a new zero-day vulnerability in iOS and iPad. The vulnerability is being tracked as CVE-2023-42824, and according to their advisory: "Apple is aware of a report that this issue may have been actively exploited against versions of iOS before iOS 16.6." CVE-2023-42824 is a kernel level vulnerability, which could be exploited by a local attacker to elevate their privileges. The following devices can be vulnerable to this exploit:

- iPhone XS and later
- iPad Pro 12.9-inch 2nd generation and later
- Pad Pro 10.5-inch
- iPad Pro 11-inch 1st generation and later
- iPad Air 3rd generation and later
- iPad 6th generation and later
- iPad mini 5th generation and later

Apple has also released updates for CVE-2023-5217, which affects iOS 17.0.3 and iPad 17.0.3 for multiple products. This vulnerability impacts the WebRTC component and can lead to heap-based buffer overflow in the VP8 compression format in libvpx. HC3 recommends following CISA's guidance, which encourages users and administrators to review the following advisory and apply the necessary updates:

- iOS 17.0.3 and iPadOS 17.0.3

Towards the end of the month, Apple released several additional advisories. HC3 recommends users follow CISA's guidance to review the following advisories and apply updates. The exploitation of these vulnerabilities could allow a threat actor to take control of an affected device.

- iOS 17.1 and iPadOS 17.1
- iOS 16.7.2 and iPad 16.7.2
- iOS 15.8 and iPad 15.8
- macOS Sonoma 14.1

- macOS Ventura 13.6.1
- macOS Monterey 12.7.1
- tvOS 17.1
- watchOS 10.1
- Safari 17.1

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

- Firefox for iOS 119
- Thunderbird 115.4.1
- Firefox ESR 115.4
- Firefox 119

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 ten security updates to address vulnerabilities in multiple products. Two were classified as "Critical" in severity, four as "High," and four as "Medium" in severity. The two critical vulnerabilities impact the Cisco Emergency Responder (CVE-2023-20101) and the Catalyst SD-WAN Manager (CVE-2023-20034, CVE-2023-20252, CVE-2023-20253, CVE-2023-20254, CVE-2023-20262). If successful, a cyber threat actor can exploit some of these vulnerabilities to take control of an affected device, system, or cause a denial-of-service condition. It should be noted that Cisco updated their October advisory for the IOS XE Software Web UI Feature on November 1, 2023, and this is now a critical vulnerability that has been actively exploited (CVE-2023-20198, CVE-2023-20273). HC3 recommends following CISA's guidance, which strongly urges users and administrators to review the following advisories and apply updates immediately:

- IOS XE Software Web UI
- Cisco Emergency Responder Static Credentials Vulnerability
- Multiple Cisco Unified Communications Products Unauthenticated API High CPU Utilization Denial of Service Vulnerability

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 seven new security notes, and two 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 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 security note for the vulnerability with a "Hot News" severity rating is as follows:

- **Security Note #2622660:** (No CVE Associated) This is an update to a security note released back on April 2018, which includes security updates for the browser control Google Chromium delivered with SAP Business Client. Product impacted: SAP Business Client, Versions - 6.5, 7.0, 7.70.

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.

VMWare

VMWare released five security updates addressing vulnerabilities in multiple products. One of these vulnerabilities was rated as critical, and the remaining were given an important rating in severity. 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-2023-0023 (CVE-2023-34048, CVE-2023-34056) 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 vCenter Server can trigger an out-of-bounds write, potentially leading to remote code execution.

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 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:

- APSB23-49: Security update available for Adobe Bridge
- APSB23-50: Security update available for Adobe Commerce
- APSB23-51: Security update available for Adobe Photoshop

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

Fortinet

Fortinet's October vulnerability advisory addressed several vulnerabilities across different Fortinet products, with the most severe being tracked as CVE-2023-40714. CVE-2023-40714 is a path traversal vulnerability and was assigned a critical rating (CVSS score of 9.7). These advisories address updates for

FortiManager, FortiOS, FortiSIEM, and FortiADC. 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-23-189
- FG-IR-23-062
- FG-IR-23-167
- FG-IR-23-352
- FG-IR-23-318
- FG-IR-23-085

Atlassian

Atlassian released a security advisory regarding two critical and twenty-six high-severity vulnerabilities in their Security Bulletin - October 17 2023. The two critical vulnerabilities are in the Confluence Data Center and Server (CVE-2023-22515), and in the Jira Service Management Data Center and Jira Service Management Server (CVE-2019-13990). According to an advisory from CISA, CVE-2023-22515 has been an actively exploited zero-day and can allow malicious cyber threat actors to obtain initial access to Confluence instances through the creation of unauthorized Confluence administrator accounts. HC3 strongly encourages that users and administrations view the advisory and apply upgrades provided by Atlassian. Additionally, a complete list of security advisories and bulletins from Atlassian can be viewed here.

SolarWinds

SolarWinds released a security update for their Access Rights Manager (ARM). This update addressed eight vulnerabilities, with three of them being rated as critical (CVE-2023-35182, CVE-2023-35185, CVE-2023-35187) and can lead to remote code execution on the "SYSTEM" of a Windows computer. This could enable an attacker to operate with the highest level of privileges available on the machine. Additional details on the vulnerabilities from the Zero Day Initiative are listed below:

- CVE-2023-35182: This flaw exists within the "createGlobalServerChannelInternal" method, which results from the lack of proper validation of user-supplied data that can result in a deserialization of untrusted data, and can allow remote attackers to execute arbitrary code.
- CVE-2023-35185: This flaw exists within the "OpenFile" method, which results from the lack of proper validation of a user-supplied path prior to using it in file operations, and can allow remote attackers to perform directory traversal, which can lead remote code execution.
- CVE-2023-35187: This flaw exists within the "OpenClientUpdateFile" method, which results from the lack of proper validation of a user-supplied path prior to using it in file operations, and can allow remote attackers to execute arbitrary code.

A complete list of the critical and high-severity vulnerabilities that were identified within the ARM software can be viewed here, and a complete list of SolarWinds security vulnerabilities can be viewed here. HC3 recommends that all users apply necessary updates and patches immediately.

NextGen Healthcare

A vulnerability was reported impacting NextGen Healthcare's Mirth Connect application. This vulnerability is an unauthenticated remote code execution flaw, tracked as CVE-2023-43208, which could be exploited to gain initial access into an environment or to compromise healthcare data. Specific information regarding this exploit is not currently available, but according to the report, all versions prior to 4.4.1 are at risk. HC3 strongly encourages that users update to the most recent version to prevent damage to the HPH sector.

F5

F5 released a security advisory in October that addresses a critical vulnerability in BIG-IP that is tracked as CVE-2023-46747. Additionally, they reported another flaw that was rated as high in severity, along with a security exposure risk. CVE-2023-46747 impacts all modules and multiple versions (listed below) of BIG-IP. This flaw can allow for an unauthenticated attacker with network access to the BIG-IP system through either the management port or self IP addresses, which could lead to the execution of arbitrary system commands. HC3 recommends that users view the F5 security advisory and make any necessary upgrades to prevent the exploitation of this vulnerability.

- 17.1.0
- 16.1.0 – 16.1.4
- 15.1.0 – 15.1.10
- 14.1.0 – 14.1.5
- 13.1.0 – 13.1.5

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

Apple Releases Security Updates for Multiple Products
https://www.cisa.gov/news-events/alerts/2023/10/26/apple-releases-security-advisories-multiple-products

Apple Releases Security Updates for iOS and iPadOS
https://www.cisa.gov/news-events/alerts/2023/10/06/apple-releases-security-updates-ios-and-ipados

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

Cisco Releases Security Advisories for Multiple Products
Cisco Releases Security Advisories for Multiple Products | CISA

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

Fortinet PSIRT Advisories
PSIRT Advisories | FortiGuard

Microsoft October 2023 Patch Tuesday fixes 3 zero-days, 104 flaws
https://www.bleepingcomputer.com/news/microsoft/microsoft-october-2023-patch-tuesday-fixes-3-zero-days-104-flaws/

Microsoft October 2023 Patch Tuesday
https://isc.sans.edu/diary/October+2023+Microsoft+Patch+Tuesday+Summary/30300/

Microsoft Month Archives: October 2023
https://msrc.microsoft.com/blog/2023/10/

Mozilla Foundation Security Advisory 2023-45
https://www.mozilla.org/en-US/security/advisories/mfsa2023-45/

Mozilla Foundation Security Advisory 2023-46
https://www.mozilla.org/en-US/security/advisories/mfsa2023-46/

Mozilla Releases Security Updates for Multiple Products
https://www.cisa.gov/news-events/alerts/2023/10/25/mozilla-releases-security-advisories-multiple-products

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

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

October Android updates fix zero-day exploited in attacks
https://www.bleepingcomputer.com/news/security/android-october-security-update-fixes-zero-days-exploited-in-attacks/

K000137368: Overview of F5 vulnerabilities (October 26, 2023)
Overview of F5 vulnerabilities (October 26, 2023)

SAP Security Patch Day – October 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

VMware Releases Security Update for Tools
VMware Releases Security Advisory for vCenter Server | CISA

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