HC3: Monthly Cybersecurity Vulnerability Bulletin
November 14, 2022 TLP: Clear Report: 202211141500

October Vulnerabilities of Interest to the Health Sector

In October 2022, 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 this month are from Microsoft, Google/Android, Apple, Oracle, Cisco, Adobe, SAP, and VMWare. A vulnerability is given the classification as a zero-day if it is actively exploited with no fix available or 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 12 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 US federal enterprise.

Vulnerabilities that are entered into this catalog are required to be patched by their associated deadline by all US executive agencies. While these requirements do not extend to the private sector, HC3 recommends all healthcare entities review 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 fixes for 84 vulnerabilities and an actively exploited Windows vulnerability. The patches released address CVEs in: Microsoft Windows and Windows Components; Azure, Azure Arc, and Azure DevOps; Microsoft Edge (Chromium-based); Office and Office Components; Visual Studio Code; Active Directory Domain Services and Active Directory Certificate Services; Nu Get Client; Hyper-V; and the Windows Resilient File System (ReFS). Thirteen of the 84 vulnerabilities fixed are classified as 'Critical' as they allow privilege elevation, spoofing, or remote code execution. The number of bugs in each vulnerability category is listed as follows:

- 39 Elevation of Privilege Vulnerabilities
- 2 Security Feature Bypass Vulnerabilities
- 20 Remote Code Execution Vulnerabilities
- 11 Information Disclosure Vulnerabilities
- 8 Denial of Service Vulnerabilities
- 4 Spoofing Vulnerabilities

The bulleted section above does not include the 12 patches that were fixed on October 3rd for CVEs in Microsoft Edge (Chromium-based).

October's Patch Tuesday also includes fixes for two publicly zero-day vulnerabilities; one actively exploited

in attacks, and one publicly disclosed. The actively exploited zero-day vulnerability fixed is tracked as CVE-2022-41033 is a Windows COM+ Event System Service Elevation of Privilege Vulnerability. If successful, a threat actor who is able to successfully exploit this vulnerability, could gain SYSTEM privileges. The publicly disclosed vulnerability is CVE-2022-41043 and it is a Microsoft Office Information Disclosure Vulnerability. If successful with their attack, a threat actor could use this vulnerability to gain access to users' authentication tokens. It is worth noting that after October's Patch Tuesday, Microsoft released security updates for two actively exploited zero-day vulnerabilities tracked as CVE-2022-41040 and CVE-2022-41082 that can be viewed by clicking here.

HC3 recommends users follow Microsoft's guidance to refer to Microsoft's Security Response Center. For a complete list of Microsoft vulnerabilities released in October and their rating click here and for all security updates click here. HC3 recommends users apply all necessary updates and patches immediately as these vulnerabilities can adversely impact the health sector.

Google/Android

Google released security updates to address 42 Android vulnerabilities. Four of these flaws are 'Critical' in severity; three of which affect Qualcomm's components. The critical Qualcomm vulnerabilities are pertaining to the WLAN component. Additional information on each is as follows:

- CVE-2022-25748 (9.8 CVSS score) and could be exploited to trigger memory corruption leading to arbitrary code execution.
- CVE-2022-25718 (9.1 CVSS score) and could allow a remote attacker to perform a machine in the middle (MitM) attack.
- CVE-2022-25720 (9.8 CVSS score) and could allow a remote attacker to execute arbitrary code on an Android device by sending it send specially crafted traffic.

CVE-2022-20419 is the fourth critical vulnerability in the Framework. In setOptions of ActivityRecord.java, there is a possible load any arbitrary Java code into launcher process due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. In addition to this, there is no user interaction required for this exploitation to occur. This impacts the following Android Versions: Android-12L Android-13Android ID: A-237290578

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 improve 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 security vulnerabilities affecting Android devices can be viewed by clicking here.

Apple

Apple released security updates to address vulnerabilities in several products. If successful, a threat actor could exploit these vulnerabilities and take control of a compromised device. HC3 recommends all users and administrators follow CISA's guidance to review Apple's security updates page for the following products and apply the necessary updates as soon as possible:

- Safari 16.1

- iOS 16.1 and iPadOS 16
- macOS Big Sur 11.7.1
- macOS Monterey 12.6.1
- macOS Ventura 13
- tvOS 16.1
- watchOS 9.1

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.

Oracle

Oracle has released their Critical Patch Update that addresses 366 vulnerabilities across multiple products. If successful with launching an attack, a threat actor could exploit some of these vulnerabilities to take control of a compromised system. HC3 recommends following CISA's guidance which encourages users and administrators to review Oracle's October 2022 Critical Patch Update and apply the necessary mitigations.

Cisco

Cisco released security updates to address vulnerabilities in multiple Cisco products including Cisco Identity Services Engine (ISE). If successful, a remote threat actor can exploit some of these vulnerabilities and take control of a compromised system. CISA encourages users and administrators to review the following advisories and apply the necessary updates:

- Cisco Identity Services Engine Unauthorized File Access Vulnerability (CVE-2022-20822)
- Cisco Enterprise NFV Infrastructure Software Improper Signature Verification Vulnerability (CVE-2022-20929)
- Cisco Expressway Series and Cisco TelePresence Video Communication Server Vulnerabilities (CVE-2022-20814 / CVE-2022-20853)

For a complete list of Cisco security advisories released, 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 recommends users and administrators follow CISA's guidance and apply necessary patches immediately.

Adobe

Adobe released several security updates to address 29 vulnerabilities across a variety of products, including Acrobat and Reader, ColdFusion, Commerce and Magento. At the time of publication, Adobe said it is not aware of active attacks against any of these flaws. If successful in launching an attack, a threat actor could exploit some of these vulnerabilities to take control of a compromised system. CISA encourages users and administrators to review the following Adobe Security Bulletins and apply necessary updates for the following:

- Adobe Cold Fusion APSB22-44
- Adobe Acrobat and Reader APSB22-46
- Adobe Commerce and Magneto Open Source APSB22-48

- Adobe Dimension APSB22-57

HC3 also recommends users follow CISA's guidance, apply the appropriate security updates and patches immediately that can be found on Adobe's Product Security Incident Response Team (PSIRT) by clicking here.

SAP

For Patch Day, SAP released 15 new security notes to address vulnerabilities affecting multiple products. If successful with launching an attack, a threat actor could exploit these vulnerabilities and take control of a compromised device or system. This month there were two vulnerabilities with a severity rating of "Hot News" which is the most severe rating. A breakdown of the security notes for vulnerabilities with a "Hot News" severity rating are as follows:

- Security Note #3242933 (CVE-2022-39802) has a 9.9 CVSS Score and a *'Hot News'* severity rating. SAP Manufacturing Execution in versions 15.1, 15.2, 15.3, allows a threat actor to exploit insufficient validation of a file path request parameter. The intended file path can be manipulated to allow arbitrary traversal of directories on the remote server. The file content within each directory can be read which may lead to information disclosure. *Product impacted*: AP Manufacturing Execution, Versions -15.1, 15.2, 15.3.

- Security Note #3239152 (CVE-2022-41204) has a 9.6 CVSS Score and a *'Hot News'* severity rating. If successful, a threat actor could change the content of an SAP Commerce (versions 1905, 2005, 2105, 2011, 2205) login page through a manipulated URL. The threat actor could inject code that allows them to redirect submissions from the affected login form to their own server which allows them to steal credentials and hijack accounts. A successful attack could compromise the Confidentiality, Integrity, and Availability of the system. *Product impacted*: SAP Commerce, Versions -1905, 2005, 2105, 2011, 2205.

For a complete list of SAP's security notes and updates for vulnerabilities released this month 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 three security advisories in October. One advisory has a 'Critical' severity rating, one 'Important,' and the third has a 'Moderate' severity rating. Additional information on the more severe vulnerabilities are as follows:

- VMSA-2022-0027.1 - VMware Cloud Foundation updates that address multiple vulnerabilities (CVE-2021-39144, CVE-2022-31678). Due to an unauthenticated endpoint that leverages XStream for input serialization in VMware Cloud Foundation (NSX-V), a threat actor could gain remote code execution in the context of 'root' on the appliance. This advisory has a maximum CVSSv3 base of 9.8 and a 'Critical' severity rating.

- VMSA-2022-0025 - VMware ESXi and vCenter Server updates address multiple security

vulnerabilities (CVE-2022-31680, CVE-2022-31681). A threat actor with admin access on vCenter server could exploit this vulnerability to execute arbitrary code on the underlying operating system that hosts the vCenter Server. This advisory has a maximum CVSSv3 base score of 7.2 and an 'Important' severity rating.

HC3 recommends recommend users follows VMWare's guidance and immediately apply patches listed in the 'Fixed Version' column of the 'Response Matrix' that can be accessed by clicking directly on the security advisory for VMSA-2022-0025 or VMSA-2022-0027.1.

References

Adobe Product Security Incident Response Team
https://helpx.adobe.com/security.html

Adobe Releases Security Updates for Multiple Products
https://www.cisa.gov/uscert/ncas/current-activity/2022/10/11/adobe-releases-security-updates-multiple-products

Android Security Bulletin— October 2022
https://source.android.com/docs/security/bulletin/2022-10-01

Android vulnerabilities could allow arbitrary code execution
https://www.malwarebytes.com/blog/news/2022/10/vulnerabilities-in-google-android-could-allow-for-arbitrary-code-execution

Apple Releases Security Updates for Multiple Products
https://www.cisa.gov/uscert/ncas/current-activity/2022/10/26/apple-releases-security-updates-multiple-products

Apple Releases Patch for New Actively Exploited iOS and iPadOS Zero-Day Vulnerability
https://thehackernews.com/2022/10/apple-releases-patch-for-new-actively.html

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

Cisco Releases Security Updates for Multiple Products
https://www.cisa.gov/uscert/ncas/current-activity/2022/10/06/cisco-releases-security-updates-multiple-products

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

Microsoft October 2022 Patch Tuesday fixes zero-day used in attacks, 84 flaws
https://www.bleepingcomputer.com/news/microsoft/microsoft-october-2022-patch-tuesday-fixes-zero-day-used-in-attacks-84-flaws/

Microsoft October 2022 Patch Tuesday Fixes 84 Flaws, Including Zero-Day

https://www.infosecurity-magazine.com/news/microsoft-october-patch-tuesday/

Microsoft Patch Tuesday, October 2022 Edition
https://krebsonsecurity.com/2022/10/microsoft-patch-tuesday-october-2022-edition/

Microsoft Patch Tuesday: 84 new vulnerabilities
https://www.zdnet.com/article/microsoft-patch-tuesday-84-new-vulnerabilities/

Microsoft Patch Tuesday by Morphus Labs
https://patchtuesdaydashboard.com/

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

Microsoft October 2022 Patch Tuesday
https://isc.sans.edu/diary/October%202022%20Microsoft%20Patch%20Tuesday/29138

Microsoft Security Updates
https://msrc.microsoft.com/update-guide/releaseNote/2022-Oct

October 2022 Patch Tuesday: 13 Critical CVEs, One Actively Exploited Bug, ProxyNotShell Still Unpatched
https://www.crowdstrike.com/blog/patch-tuesday-analysis-october-2022/

Pixel Update Bulletin - October 2022
https://source.android.com/docs/security/bulletin/pixel/2022-10-01

Oracle Releases October 2022 Critical Patch Update
https://www.cisa.gov/uscert/ncas/current-activity/2022/10/19/oracle-releases-october-2022-critical-patch-update

SAP Patches Critical Vulnerabilities in Commerce, Manufacturing Execution Products
https://www.securityweek.com/sap-patches-critical-vulnerabilities-commerce-manufacturing-execution-products

SAP Security Patch Day – October 2022
https://securitybridge.com/sap-patchday/sap-security-patch-day-october-2022/

SAP Security Patch Day: October 2022
https://securityboulevard.com/2022/10/sap-security-patch-day-october-2022/

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

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