HC3: Monthly Cybersecurity Vulnerability Bulletin
October 25, 2022 TLP: White Report: 202210251500

September Vulnerabilities of Interest to the Health Sector

In September 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, 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 25 vulnerabilities in September 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 79 vulnerabilities. Of these flaws, five allow remote code execution and are classified as "Critical," which is one of the most severe types of vulnerabilities.

The number of bugs in each vulnerability category is listed as follows:

- 18 Elevation of Privilege Vulnerabilities
- 1 Security Feature Bypass Vulnerabilities
- 30 Remote Code Execution Vulnerabilities
- 7 Information Disclosure Vulnerabilities
- 7 Denial of Service Vulnerabilities
- 16 Edge - Chromium Vulnerabilities

The bulleted section does not include the 16 vulnerabilities fixed in Microsoft Edge before Patch Tuesday. This Patch Tuesday included fixes for two publicly disclosed zero-day vulnerabilities, with one actively exploited in attacks. CVE-2022-37969 (CVSS7.8), the actively exploited zero-day vulnerability fixed, is a Windows Common Log File System Driver Elevation of Privilege Vulnerability. According to Microsoft's advisory, "An attacker who successfully exploited this vulnerability could gain SYSTEM privileges." CVE-2022-23960 is the other publicly disclosed flaw and it is a Cache Speculation Restriction vulnerability. In addition to this, researchers also identified two zero-day vulnerabilities in Microsoft Exchange that were being actively exploited in the wild. If successful with their efforts, threat actors could gain initial access

through the following flaws: CVE-2022-41040 which is a Server-Side Request Forgery (SSRF) vulnerability and CVE-2022-41082 which allows remote code execution (RCE) when PowerShell is accessible to the attacker. According to Microsoft, in a successful attack using CVE-2022-41040 an authenticated threat actor will have the ability to remotely trigger CVE-2022-41082. With this attack, authenticated access to the vulnerable Microsoft Exchange Server is necessary for a threat actor to successfully exploit either of the two vulnerabilities.

HC3 recommends users follow Microsoft's guidance to refer to Microsoft Security Response Center's post and for additional information on mitigations that Microsoft currently has in place click here. To view the complete list of Microsoft vulnerabilities released in September 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 Chrome 105.0.5195.102 for Windows, Mac, and Linux users to address a single high-severity security flaw, the sixth Chrome zero-day exploited in attacks patched this year. The new version will roll out in the Stable Desktop channel which Google states will eventually reach all users; to see the entire list of changes in this build click here.

CVE-2022-3075 is the zero-day vulnerability fixed with this month's updates. This is a high severity vulnerability caused by insufficient data validation in Mojo which is a collection of runtime libraries that facilitates message passing across arbitrary inter- and intra-process boundaries. Google acknowledged that this zero-day was exploited in the wild and said, "access to bug details and links may be kept restricted until a majority of users are updated with a fix."

HC3 recommends that users upgrade their Google Chrome web browser immediately and refer to the Android and Google Play Protect mitigations section for details on the Android security platform protections and Google Play Protect, which improve the security of the Android platform. In addition to this, users should review Google's Stable Channel Update for Desktop for more information related to this month's update. 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. A summary of the mitigations provided by the Android security platform and service protections 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 following CISA's guidance that encourages all users and administrators to review the Apple security updates page for the following products and apply the necessary updates as soon as possible:

- Safari 16
- iOS 16
- macOS Monterey 12.6
- macOS Big Sur 11.7
- iOS 15.7 and iPadOS 15.7

For a complete list of the latest Apple security and software updates click here. HC3 recommends all users install updates and apply patches immediately. According to Apple, after a software update is installed for iOS, iPadOS, tvOS, and watchOS it cannot be downgraded to the previous version.

Cisco

Cisco released 31 security updates this month to address vulnerabilities in multiple Cisco products. 16 of these flaws have a "High" severity rating, 13 "Medium," and one is classified as "Informational." If successful, a threat actor could exploit some of these vulnerabilities and take control of an affected system. HC3 recommends following CISA's guidance which encourages users and administrators to review advisories for Cisco SD-WAN vManage Software Unauthenticated Access to Messaging Services along with NVIDIA Data Plane Development Kit and apply the necessary updates.

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

For September's Patch Tuesday, Adobe released several security updates to address vulnerabilities in their products. If successful in launching an attack, a threat actor could exploit some of these vulnerabilities to take control of a compromised device or system. CISA encourages users and administrators to review the following Adobe Security Bulletins and apply necessary updates for the following:

- Experience Manager APSB22-40
- Bridge APSB22-49
- InDesign APSB22-50
- Photoshop APSB22-52
- InCopy APSB22-53
- Animate APSB22-54
- Illustrator APSB22-55

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

SAP released 16 new and updated security patches to address vulnerabilities affecting multiple products. If successful a threat actor could exploit some of these vulnerabilities to take control of a compromised system. This month there was one vulnerability with severity a rating of "Hot News" which is the most severe rating and is an update to a previously released security note. In addition to this, there were six vulnerabilities with a "High" severity rating and 9 classified as "Medium." A breakdown of some advisories for vulnerabilities with a "Hot News" and a "High" severity rating are as follows:

- Security Note#2622660 (Update) (10 CVSS Score, Hot News severity rating) - Security updates for the browser control Google Chromium delivered with SAP Business Client.
- Security Note#3102769 (Update) or CVE-2021-42063 (8.8 CVSS score, High severity rating) - This is a Cross-Site Scripting (XSS) vulnerability in SAP Knowledge Warehouse.

- Security Note# 3226411 (Update) or CVE-2022-35291 (8.1 CVSS score, High severity rating) – This is a Privilege escalation vulnerability in SAP SuccessFactors attachment API for Mobile Application (Android & iOS)
- Security Note# 2998510 (Update) or CVE-2022-28214 (7.8 CVSS score, High severity rating) – This is a Central Management Server Information Disclosure in Business Intelligence Update.
- Security Note#3223392 or CVE-2022-35292(7.8 CVSS score, High severity rating) – This is a Windows Unquoted Service Path issue in SAP Business One.
- Security Note#3217303 or CVE-2022-39014 (7.7 CVSS score, High severity rating) – This is an Information Disclosure vulnerability in SAP BusinessObjects Business Intelligence Platform (CMC).

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 one security advisory this month. VMSA-2022-0024.1 (CVSS 7.0) is an update for CVE-2022-31676 and has an "Important" severity rating. This local privilege escalation vulnerability impacts VMWare Tools. If successful, a malicious threat actor that can gain local non-administrative access to the Guest OS can escalate privileges as a root user in the virtual machine.

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 here.

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/2022/09/13/adobe-releases-security-updates-multiple-products

Android Security Bulletin—September 2022
https://source.android.com/docs/security/bulletin/2022-09-01

Apple fixes eighth zero-day used to hack iPhones and Macs this year
https://www.bleepingcomputer.com/news/security/apple-fixes-eighth-zero-day-used-to-hack-iphones-and-macs-this-year/

Apple Releases Security Updates for Multiple Products
https://www.cisa.gov/uscert/ncas/current-activity/2022/09/13/apple-releases-security-updates-multiple-products

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

HC3: Monthly Cybersecurity Vulnerability Bulletin
October 25, 2022 TLP: White Report: 202210251500

Cisco Releases Security Updates for Multiple Products
https://www.cisa.gov/uscert/ncas/current-activity/2022/09/08/cisco-releases-security-updates-multiple-products

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

Customer Guidance for Reported Zero-day Vulnerabilities in Microsoft Exchange Server
https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/

Google Chrome emergency update fixes new zero-day used in attacks
https://www.bleepingcomputer.com/news/security/google-chrome-emergency-update-fixes-new-zero-day-used-in-attacks/

Google's September 2022 security patch is here for Pixel phones with fixes for wireless charging
https://www.androidpolice.com/pixel-september-2022-security-patch/

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

Microsoft says two new Exchange zero-day bugs under active attack, but no immediate fix
https://techcrunch.com/2022/09/30/microsoft-exchange-zero-days/

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

Microsoft September 2022 Patch Tuesday
https://isc.sans.edu/forums/diary/Microsoft+September+2022+Patch+Tuesday/29044

Microsoft September 2022 Patch Tuesday fixes zero-day used in attacks, 63 flaws
https://www.bleepingcomputer.com/news/microsoft/microsoft-september-2022-patch-tuesday-fixes-zero-day-used-in-attacks-63-flaws/

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

Mojo Docs
https://chromium.googlesource.com/chromium/src/+/HEAD/mojo/README.md#system-overview

Pixel Update Bulletin—September 2022
https://source.android.com/docs/security/bulletin/pixel/2022-09-01

SAP Security Patch Day-September 2022
https://securitybridge.com/sap-patchday/sap-security-patch-day-september-2022/

HC3: Monthly Cybersecurity Vulnerability Bulletin
October 25, 2022 TLP: White Report: 202210251500

SECURITY ALERT: Attack Campaign Utilizing Microsoft Exchange 0-Day (CVE-2022-41040 and CVE-2022-41082)
https://success.trendmicro.com/dcx/s/solution/000291651?language=en_US

Stable Channel Update for Desktop
https://chromium.googlesource.com/chromium/src/+log/105.0.5195.52..105.0.5195.102?pretty=fuller&n=10000

Two Microsoft Exchange zero-days exploited by attackers (CVE-2022-41040, CVE-2022-41082)
https://www.helpnetsecurity.com/2022/09/30/cve-2022-41040-cve-2022-41082/

Unpatched Microsoft Exchange Zero-Day actively exploited in the wild
https://securityaffairs.co/wordpress/136433/hacking/microsoft-exchange-zero-day-2.html

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

Wormable Flaw, 0days Lead Sept. 2022 Patch Tuesday
https://krebsonsecurity.com/2022/09/wormable-flaw-0days-lead-sept-2022-patch-tuesday/

Zero-Day Exploit in-the-Wild Exchange
Warning: New Attack Campaign Utilized a New 0-Day RCE Vulnerability on Microsoft Exhange Server
https://www.gteltsc.vn/blog/warning-new-attack-campaign-utilized-a-new-0day-rce-vulnerability-on-microsoft-exchange-server-12715.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