HC3: Monthly Cybersecurity Vulnerability Bulletin
June 8, 2022 TLP: White Report: 202206081200

May Vulnerabilities of Interest to the Health Sector

In May 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, Apple, Cisco, Mozilla, SAP, and VMWare. HC3 recommends patching all vulnerabilities with special consideration to the risk management posture of the organization.

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 83 vulnerabilities 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 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 patches for three zero-day vulnerabilities, one of which is being actively exploited, and a total of 75 vulnerabilities. Products impacted by May's security update include the Windows OS and several of its components: the .NET and Visual Studio platforms, Office and its components, Exchange Server, BitLocker, Remote Desktop Client, NTFS, and Microsoft Edge. Eight of the 75 CVEs are classified as "Critical", as they allow either remote code execution or elevation of privileges. The number of bugs in each vulnerability category are as follows:

- 21 Elevation of Privilege Vulnerabilities
- 4 Security Feature Bypass Vulnerabilities
- 26 Remote Code Execution Vulnerabilities
- 17 Information Disclosure Vulnerabilities
- 6 Denial of Service Vulnerabilities
- 1 Spoofing Vulnerability
- 0 Edge - Chromium Vulnerabilities

According to Microsoft's recommendation, administrators should read the PetitPotam NTLM Relay advisory for additional information on how to mitigate these types of attacks.

The two publicly exposed zero-days for this month are a denial-of-service vulnerability in Hyper-V, and a new remote code execution vulnerability in Azure Synapse and Azure Data Factory:

- CVE-2022-22713 - Windows Hyper-V Denial of Service Vulnerability
- CVE-2022-29972 - Insight Software: Magnitude Simba Amazon Redshift ODBC Driver

HC3: Monthly Cybersecurity Vulnerability Bulletin
June 8, 2022 TLP: White Report: 202206081200

Some severe vulnerabilities resolved this month are as follows:

- CVE-2022-26925: This is the only vulnerability listed as being actively exploited in May. Classified as “Important", this flaw allows malicious threat actors to "call a method on the LSARPC interface and coerce the domain controller to authenticate to the attacker using NTLM”. Although this vulnerability has a CVSS severity rating of 8.1, Microsoft noted that the severity rating could be bumped up to 9.8 if combined with NTLM relay attacks. This month’s patch addresses the vulnerability by detecting and denying anonymous connection attempts in LSARPC.

- CVE-2022-26923: This vulnerability is classified as "Critical" and exploits the issuance of certificates by inserting crafted data into a certificate request, which allows a threat actor to obtain a certificate that can authenticate a domain controller with a high-level of privilege. If a threat actor can gain unauthorized authentication, it allows that individual to become a domain administrator within any domain running Active Directory Certificate Services.

- CVE-2022-30190 – This vulnerability, also known as "Follina”, affects the Microsoft Support Diagnostic Tool (MSDT) in Windows. This month, Microsoft reported active exploitation of this vulnerability in the wild. If successful, a remote unauthenticated threat actor could exploit this vulnerability and take control of the targeted system. Microsoft released workaround guidance to address this remote code execution (RCE) vulnerability. HC3 recommends all users follow CISA’s guidance which is to review Microsoft's Guidance for CVE-2022-30190 Microsoft Support Diagnostic Tool Vulnerability and apply the necessary workaround.

To view the complete list of Microsoft vulnerabilities released in May and their rating, click here, and for all security updates, click here. HC3 recommends patching and testing immediately, as all vulnerabilities can adversely impact the health sector.

Google/Android

Google addressed 36 vulnerabilities, including one actively exploited vulnerability that is a privilege escalation flaw located in the Linux Kernel, also known as “The Dirty Pipe.” This vulnerability impacts newer Android devices that run versions Android 12 and onwards. Android also addressed 15 high-severity and one critical-severity vulnerability within Qualcomm components, three high-severity issues in MediaTek components, and two denial-of-service vulnerabilities in the Android System. Google also released a Chrome security update to address 32 issues: one is rated “Critical” and eight are rated “High” severity. The “Critical “severity vulnerability CVE-2022-1853 affects the IndexedDB feature and the “High” severity rated vulnerabilities impact DevTools, UI foundations, and the user education function. According to Google, none of the flaws fixed in Chrome 102 have been exploited. Google also addressed 13 vulnerabilities in Chrome v101.0.4951.61 for Android earlier in the month, eight of those vulnerabilities are rated as “High” in severity.

HC3 recommends that users 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. 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.

HC3: Monthly Cybersecurity Vulnerability Bulletin
June 8, 2022 TLP: White Report: 202206081200

Apple

Apple released security updates for several vulnerabilities in multiple products this month. One vulnerability of note this month is CVE-2022-22675. This vulnerability affects watchOS, tvOS, and macOS Big Sur. According to researchers, this actively exploited vulnerability was patched in this month's security updates. HC3 recommends users follows CISA's guidance that encourages users and administrators to review Apple security updates for the following products and apply the necessary updates.

- watchOS 8.6
- tvOS 15.3
- macOS Catalina
- macOS Big Sur 11.6.6
- macOS Monterey 12.4
- iOS 15.5 and iPad OS 15.5
- Xcode 13.4

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 a total of 18 security advisories. One security advisory has a "Critical" severity rating, and one security advisory has a "High" severity rating. The Critical security advisory addresses multiple vulnerabilities found in Cisco Enterprise NFV Infrastructure Software(NFVIS): CVE-2022-20777, CVE-2022-20779, CVE-2022-20780. If these CVEs are exploited, it could allow a threat actor to escape from the guest virtual machine (VM) to a host machine and inject commands that execute at the root level, or possibly leak system data from the host machine to the virtual machine.

For a complete list of security advisories released, visit the Cisco Security Advisories page by clicking here. Cisco also provides free software updates that address the vulnerabilities listed in their security advisory. HC3 recommends users and administrators apply necessary patches immediately.

Mozilla

Mozilla released updates to address seven security advisories: six with "High" severity ratings and one with a "Critical" severity rating. The following "Critical and High" severity security advisories address vulnerabilities fixed in following products:

- *Critical Severity* - MFSA 2022-19: Firefox 100.0.2, Firefox for Android 100.3.0, Firefox ESR 91.9.1, and Thunderbird 91.9.1.
- *High Severity* - MFSA 2022-22: Thunderbird 91.10, MFSA 2022-21: Firefox ESR 91.10, MFSA 2022-20: Firefox 101, MFSA 2022-18: Thunderbird 91.9, MFSA 2022-17: Firefox ESR 91.9, MFSA 2022-16: Firefox 100

HC3 recommends that all users review Mozilla security advisories and apply the necessary patches immediately.

SAP

SAP released eight new security notes and updated four; this includes three that address the recent Spring4Shell vulnerability in more products. The Spring4Shell vulnerability tracked as CVE-2022-22965 ("Hot News," 9.8 CVSS score) impacts the Spring Java framework. If a threat actor is successful, this could lead to remote code execution, and some security researchers have reported observing attempts to exploit this vulnerability in the wild. Additionally, SAP also published three "Hot News" rated security notes for Spring4Shell. Further updates included two high-priority security notes that addressed CVE-2022-27656 (8.3 CVSS score), a cross-site scripting (XSS) issue in the administration UI of Web Dispatcher and Netweaver and CVE-2022-28214 (7.8 CVSS score), which is an information disclosure in BusinessObjects.

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 updates for nine vulnerabilities in its products, some of which could be exploited by threat actors to launch remote code execution attacks. Four of these vulnerabilities have a severity rating of "Critical," one as "Important," and two as "Moderate". A couple of critical vulnerabilities of note this month are:

- CVE-2022-22972 (9.8 CVSS score) - VMware Workspace ONE Access, Identity Manager and vRealize Automation contain an authentication bypass vulnerability that affects local domain users. If successful, a threat actor with network access to the UI may be able to obtain administrative access without needing authentication.

- CVE-2022-22973 (7.8 CVSS score) - VMware Workspace ONE Access and Identity Manager contain a privilege escalation vulnerability. If successful, a threat actor with local access can escalate privileges to 'root'.

HC3 recommends VMWare users check for frequent updates, keep software updated, and to apply patches immediately. For a complete list of this month's VMWare Security advisories, click here.

HC3: Monthly Cybersecurity Vulnerability Bulletin
June 8, 2022 TLP: White Report: 202206081200

Recently Published Information

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

Apple Releases Security Updates for Multiple Products
https://www.cisa.gov/uscert/ncas/current-activity/2022/05/17/apple-releases-security-updates-multiple-products

Cisco Security Advisories
https://tools.cisco.com/security/center/publicationListing.x?product=Cisco&last_published=2022%20May&sort=-day_sir#~Vulnerabilities

May 2022 Patch Tuesday | Microsoft Releases 75 Vulnerabilities with 8 Critical; Adobe Releases 5 Advisories, 18 Vulnerabilities with 16 Critical
https://blog.qualys.com/vulnerabilities-threat-research/2022/05/10/may-2022-patch-tuesday

Microsoft Patch Tuesday for May 2022 — Snort rules and prominent vulnerabilities
https://blog.talosintelligence.com/2022/05/microsoft-patch-tuesday-for-may-2022.html

Microsoft May 2022 Patch Tuesday
https://isc.sans.edu/forums/diary/Microsoft+May+2022+Patch+Tuesday/28632/

Microsoft May 2022 Patch Tuesday fixes 3 zero days, 75 flaws
https://www.bleepingcomputer.com/news/microsoft/microsoft-may-2022-patch-tuesday-fixes-3-zero-days-75-flaws/

Microsoft May 2022 Patch Tuesday fixes 7 critical vulnerabilities, 67 others
https://www.zdnet.com/article/microsoft-may-2022-patch-tuesday-seven-critical-vulnerabilities/

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

Microsoft releases fixes for Azure flaw allowing RCE attacks
https://www.bleepingcomputer.com/news/security/microsoft-releases-fixes-for-azure-flaw-allowing-rce-attacks/

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

The May 2022 Security Update Review
https://www.zerodayinitiative.com/blog/2022/5/10/the-may-2022-security-update-review

Patch Tuesday May 2022 – Microsoft Pledges Fixes and Improvements for Azure Synapse Pipeline and Azure Data Factory
https://heimdalsecurity.com/blog/patch-tuesday-may-2022/

SAP Security Patch Day – May 2022
https://securitybridge.com/sap-patchday/sap-security-patch-day-may-2022-2/

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

Contact Information

If you have any additional questions, please 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