HC3: Monthly Cybersecurity Vulnerability Bulletin
June 14, 2023 TLP:CLEAR Report: 202306141200

May Vulnerabilities of Interest to the Health Sector

In May 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 May are from Microsoft, Google/Android, Apple, Mozilla, SAP, Cisco, Fortinet, VMWare, and MOVEit. 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

MOVEit Transfer Critical Vulnerability

A critical vulnerability was discovered in Progress/IPswitch's MOVEit Transfer software. MOVEit is a managed file transfer software that encrypts files and uses secure File Transfer Protocols to transfer data with automation, analytics and failover options. Tracked as CVE-2023-34362, this vulnerability could lead to escalated privileges and potential unauthorized access to the environment. HC3 recommends that all MOVEit Transfer software users protect their MOVEit Transfer environment by taking immediate action following Progress' remediation guidance, which can be viewed by clicking here.

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 19 vulnerabilities in May 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 issued security updates to fix 38 vulnerabilities and two actively exploited zero-day vulnerability in May. Six of these vulnerabilities have been classified as 'Critical,' which is one of the most severe types of vulnerabilities, as they allow remote code execution. The number of bugs in each vulnerability category is listed as follows:

- 8 Elevation of Privilege Vulnerabilities
- 4 Security Feature Bypass Vulnerabilities
- 12 Remote Code Execution Vulnerabilities
- 8 Information Disclosure Vulnerabilities
- 5 Denial of Service Vulnerabilities

- 1 Spoofing Vulnerability

May's Patch Tuesday had the lowest number of resolved vulnerabilities for Microsoft, with only thirty-eight vulnerabilities fixed; this is not including eleven Microsoft Edge vulnerabilities fixed on May 5th.

May's Patch Tuesday addressed three zero-day vulnerabilities, with two exploited in attacks and one publicly disclosed. Additional information on the two actively exploited zero-day vulnerabilities is as follows:

- CVE-2023-29336 – This is a Win32k Elevation of Privilege vulnerability with a CVSS score of 7.8. Microsoft has fixed this privilege elevation vulnerability in the Win32k Kernel driver that elevates privileges to SYSTEM, which is Windows' highest user privilege level. A threat actor who successfully exploits this vulnerability could gain SYSTEM privileges.
- CVE-2023-24932 – This is a Secure Boot Security Feature Bypass vulnerability with a CVSS score of 6.2. Microsoft has fixed this Secure Boot bypass that is weaponized by the BlackLotus UEFI bootkit to exploit CVE-2022-21894 (aka Baton Drop), which was resolved in January 2022.

Microsoft also released an update for one publicly disclosed zero-day that was not actively exploited. This is tracked as CVE-2023-29325 and is a Windows OLE Remote Code Execution vulnerability. According to Microsoft, "In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted email to the victim."

For a complete list of Microsoft vulnerabilities released in May and their rating, click here, and for all security updates, click here. HC3 recommends 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 released security updates in May for Android devices with fixes for over 47 vulnerabilities. While there were no critical flaws addressed, there were high and moderate severity flaws, with the worst vulnerability potentially leading to privilege escalation if a threat actor is able to gain physical access to a target's device. Every month, security updates are released in two parts. The first part of the update arrived as the 2023-05-01 security patch level, and 16 vulnerabilities were resolved in the Android System and Framework. The second part of Android's security update arrived on devices as the 2023-05-05 security patch level. This security update included fixes for 29 vendor-specific vulnerabilities, and two Pixel-specific flaws were addressed as well. One of Android's most notable security updates released this month was a patch for a high-severity vulnerability exploited as a zero-day to install commercial spyware on compromised devices. Tracked as CVE-2023-0266, this flaw is a use-after-free weakness in the Linux Kernel sound subsystem that may result in privilege escalation without requiring user interaction. Google also released Chrome version 101.0.4951.64 for Windows, Linux, and Mac. This version addresses vulnerabilities that a threat actor could exploit to take control of a compromised system. HC3 recommends all users follow CISA's guidance to review the Chrome Release Note and apply the necessary update. HC3 also 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 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 on vulnerabilities affecting Android devices can be viewed by clicking here.

Apple

This month, CISA ordered federal agencies to address three recently patched zero-day flaws affecting Apple's iPhones, Macs, and iPads based on evidence of active exploitation. The vulnerabilities found in the WebKit browser engine are tracked as CVE-2023-32409, CVE-2023-28204, and CVE-2023-32373. If successful with exploitation, threat actors have the ability to escape the browser sandbox, access sensitive information on a compromised device, and achieve arbitrary code execution. According to CISA: "These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise." HC3 recommends all users and administrators follow CISA's guidance which "encourages users and administrators to review the following advisories and apply the necessary updates":

- Apple Multiple Products WebKit Sandbox Escape Vulnerability (CVE-2023-32409)
- Apple Multiple Products WebKit Out-of-Bounds Read Vulnerability (CVE-2023-28204)
- Apple Multiple Products WebKit Use-After-Free Vulnerability (CVE-2023-32373)

For the first time ever, Apple released a Rapid Security Response to owners of the devices running iOS 16.4.1 or later, iPadOS 16.4.1 or later, or macOS Ventura 13.3.1 or later. Apple Rapid Security Response was released about a year ago, and is a security-focused feature that makes user devices automatically install security patches as they are made available. 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 for vulnerabilities affecting multiple Mozilla products, including in Thunderbird, Firefox, and Firefox ESR. If successful, a threat actor could exploit these vulnerabilities and take control of a compromised device or system. HC3 encourages all users to follow CISA's guidance, which encourages all users to review the following advisories and apply the necessary updates:

- Firefox 113 Mozilla Foundation Security Advisory 2023-16
- Firefox ESR 102.11 Mozilla Foundation Security Advisory 2023-17
- Thunderbird 102.11 Mozilla Foundation Security Advisory 2023-18

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.

SAP

SAP released 18 new security notes and six updates to previously issued 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. There were also

nine flaws rated as "High, 10 "Medium," and three "Low" in severity. A breakdown of some security notes for vulnerabilities with "Hot News" severity rating are as follows:

- **Security Note #3328495** - (CVE-2021-44151,CVE-2021-44152,CVE-2021-44153,CVE-2021-44154,CVE-2021-44155) has a 9.8 CVSS score and 'Hot News' severity rating. Multiple vulnerabilities associated with Reprise License Manager 14.2 component used with SAP 3D Visual Enterprise License Manager. Product(s) impacted: SAP 3D Visual Enterprise License Manager, Version–15.
- **Security Note #3307833** - (CVE-2023-28762) has a 9.1 CVSS score and a 'Hot News' severity rating. Information Disclosure vulnerabilities in SAP BusinessObjects Intelligence Platform. Product(s) impacted: SAP BusinessObjects Intelligence Platform, Versions–420,430.

For a complete list of SAP's security notes and updates for vulnerabilities released in May, 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.

Cisco

Cisco released security advisories for vulnerabilities affecting multiple Cisco products. Two advisories were rated "Critical," two as "High," and 12 as "Medium." Additional information on the "Critical" security advisories are as follows:

- Cisco Small Business Series Switches Buffer Overflow Vulnerabilities has a CVSS score of 9.8. A remote threat actor could exploit these vulnerabilities to cause a denial-of-service condition or execute arbitrary code with root privileges on an affected device. Vulnerabilities for this advisory are: CVE-2023-20024, CVE-2023-20156, CVE-2023-20157, CVE-2023-20158, CVE-2023-20159, CVE-2023-20160, CVE-2023-20161, CVE-2023-20162, and CVE-2023-20189.
- Cisco SPA112 2-Port Phone Adapters Remote Command Execution Vulnerability (CVE-2023-20126) has a CVSS score of 9.8. This is a vulnerability in the web-based management interface of Cisco SPA112 2-Port Phone Adapters that could allow an unauthenticated, remote threat actor to execute arbitrary code on an affected device. This is caused by a missing authentication process within the firmware upgrade function. If successful, a remote threat actor could exploit this vulnerability by upgrading an affected device to a crafted version of firmware and execute arbitrary code on the affected device with full privileges.

Currently there are no workarounds to address these vulnerabilities. For a complete list of Cisco security advisories released in May, 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.

Fortinet

Fortinet's May vulnerability advisory addressed two "High, four "Medium," and three "Low" rated vulnerabilities across different Fortinet products, including FortiADC, FortiNAC, FortiOS and FortiProxy. Additional information on the "High" rated vulnerabilities for this month are as follows:

- FG-IR-22-297(CVE-2023-27999) has a CVSSv3 score of 7.6. This is an improper neutralization of special elements used in an OS command vulnerability [CWE-78] in FortiADC that could allow an

authenticated threat actor to execute unauthorized commands through specifically crafted arguments to existing commands.

- FG-IR-22-475 (CVE-2023-22640) has a CVSSv3 score of 7.1. This is an out-of-bounds write vulnerability [CWE-787] in sslvpnd of FortiOS and FortiProxy that could allow an authenticated threat actor to achieve arbitrary code execution through specifically crafted requests.

HC3 recommends users follow CISA's guidance, which encourages users and administrators to review Fortinet's May 2023 Vulnerability Advisories page for additional information, and apply all recommended updates and patches immediately. For a complete list of vulnerabilities addressed in May, click here to view FortiGuard Labs' Vulnerability Advisories page.

VMWare

VMWare released three security advisories; one rated "Important" (VMSA-2023-0009) and two rated "Moderate"(VMSA-2023-0010, VMSA-2023-0011). If successful, a threat actor could exploit these vulnerabilities and take control of a compromised device or system. Additional information is as follows:

- VMSA-2023-0009 - This security advisory has a maximum CVSSv3 score of 8.8 and impacts VMware Aria Operations (formerly vRealize Operations). This update addresses multiple Local Privilege Escalations and a Deserialization issue (CVE-2023-20877, CVE-2023-20878, CVE-2023-20879, CVE-2023-20880).
- VMSA-2023-0010 - This security advisory has a maximum CVSSv3 score of 4.3 and impacts NSX-T. This update addresses a cross-site scripting vulnerability (CVE-2023-20868).
- VMSA-2023-0011 - This security advisory has a maximum CVSSv3 score of 6.1 and impacts VMware Workspace ONE Access (Access), VMware Identity Manager (vIDM), and VMware Cloud Foundation (Cloud Foundation). This update addresses an Insecure Redirect Vulnerability (CVE-2023-20884).

For a complete list of VMWare's security advisories, click here. HC3 recommends users follow VMWare's guidance for each, 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.

References

Android Security Bulletins
https://source.android.com/security/bulletin

Android's May security update is rolling out now to Google Pixel phones
https://www.androidpolice.com/android-may-2023-security-google-pixel/

Android Security Bulletin—May 2023
https://source.android.com/docs/security/bulletin/2023-05-01

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

CISA Adds Three Known Exploited Vulnerabilities to Catalog
https://www.cisa.gov/news-events/alerts/2023/05/22/cisa-adds-three-known-exploited-vulnerabilities-catalog

Cisco phone adapters vulnerable to RCE attacks, no fix available
https://www.bleepingcomputer.com/news/security/cisco-phone-adapters-vulnerable-to-rce-attacks-no-fix-available/

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

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

FortiGuard Labs PSIRT Advisories
https://www.fortiguard.com/psirt

FortiGuard Labs May 2023 Vulnerability Advisories
https://www.fortiguard.com/psirt-monthly-advisory/may-2023-vulnerability-advisories

Google Chrome Releases: Stable Channel Update for Desktop
https://chromereleases.googleblog.com/2022/05/stable-channel-update-for-desktop_10.html

Microsoft May 2023 Patch Tuesday
https://isc.sans.edu/diary/rss/29826

Microsoft May 2023 Patch Tuesday fixes 3 zero-days, 38 flaws
https://www.bleepingcomputer.com/news/microsoft/microsoft-may-2023-patch-tuesday-fixes-3-zero-days-38-flaws/

Microsoft's May Patch Tuesday Fixes 38 Flaws, Including 2 Exploited Zero-Day Bugs
https://thehackernews.com/2023/05/microsofts-may-patch-tuesday-fixes-38.html

Microsoft Security Response Center May 2023
https://msrc.microsoft.com/blog/2023/05/

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

Microsoft's Security Response Center (May 2023)
https://msrc.microsoft.com/blog/2023/05/

Microsoft Patch Tuesday by Morphus Labs

https://patchtuesdaydashboard.com/

Microsoft Patch Tuesday, May 2023 Edition
https://krebsonsecurity.com/2023/05/microsoft-patch-tuesday-may-2023-edition/

MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362)
https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023

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

New Android updates fix kernel bug exploited in spyware attacks
https://www.bleepingcomputer.com/news/security/new-android-updates-fix-kernel-bug-exploited-in-spyware-attacks/

SANS Microsoft May 2023 Patch Tuesday
https://isc.sans.edu/diary/Microsoft+May+2023+Patch+Tuesday/29826/

SAP Security Patch Day – May 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 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