HC3: Monthly Cybersecurity Vulnerability Bulletin
July 13, 2022 TLP: White Report: 202207131000

June Vulnerabilities of Interest to the Health Sector

In June 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, Mozilla, Intel and SAP. 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 49 vulnerabilities in June 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 fixes for 55 vulnerabilities, new Intel MMIO flaws, and fixes for the widely exploited Windows 'Follina' MSDT zero-day vulnerability tracked as CVE-2022-30190 this month. Microsoft's official guidance for this vulnerability can be viewed by clicking here. Of the 55 vulnerabilities, there are three that allow remote code execution, are classified as 'Critical' and 52 are classified as 'Important.' In addition to this, five Microsoft Edge Chromium updates were released earlier in the month bringing the total to 60 vulnerabilities addressed in June. The breakdown of types of vulnerabilities in this month's report are as follows:

- 12 Elevation of Privilege Vulnerabilities
- 1 Security Feature Bypass Vulnerabilities
- 27 Remote Code Execution Vulnerabilities
- 11 Information Disclosure Vulnerabilities
- 3 Denial of Service Vulnerabilities
- 1 Spoofing Vulnerability

Some of the most severe vulnerabilities resolved in this update are:

- CVE-2022-30136 (9.8 CVSS score) is a Windows Network File System RCE vulnerability. With this flaw, threat actors need to make an unauthenticated, crafted call to a Network File System (NFS) service to trigger the bug.
- CVE-2022-30163: (8.5 CVSS score) is a Windows Hyper-V RCE vulnerability exploitable through a specially crafted application on a Hyper-V guest session.
- CVE-2022-30139: (7.5 CVSS score) is a Windows Lightweight Directory Access Protocol (LDAP) RCE vulnerability only if the MaxReceiveBuffer LDAP policy is set to a value higher than the default value.
- CVE-2022-30164: (8.4 CVSS score) is a Kerberos AppContainer security feature bypass. If successful, a threat actor could bypass the Kerberos service ticketing feature that performs user access control checks.
- CVE-2022-30157:(8.8 CVSS score) is a Microsoft SharePoint Server RCE vulnerability. With this flaw, a threat actor must be authenticated and have page creation permissions,
- CVE-2022-30165: (CVSS 8.8 score) is a Windows Kerberos EoP security flaw. It was possible to spoof the Kerberos log on process when a remote credential guard connection was made via CredSSP.

It is also important to note that Microsoft retired Internet Explorer this month. On June 15th Microsoft ended support for Internet Explorer 11. This change impacts the Windows 10 client SKU (versions 20H2 and later) as well as Windows 10 IoT (version 20H2 and later). In an effort to provide developers more time to modernize their IE applications, IE Mode will be maintained in Microsoft Edge until at least 2029. To view the complete list of Microsoft vulnerabilities released in June 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

For the month of June, Google released security updates for Android devices running OS versions 10, 11, and 12, fixing 41 vulnerabilities, and five listed with a “critical” rating. Security updates for this vendor is separated in two parts. The first release or patch level on June 1st contains patches for Android system and framework components and the second patch level, June 5th, includes updates for kernel and third-party vendor closed source components. CVE-2022-20210 is a standout in the group of 5 critically rated vulnerabilities. This flaw is a remote code execution vulnerability that a malicious actor could leverage without very demanding prerequisites. This is significant because remote code execution vulnerabilities are severe and could lead to high-level system compromise, information disclosure, or possibly allow a threat actor to completely takeover a targeted device. CVE-2022-20140 and CVE-2022-20145 are both critical-severity escalation of privilege flaws that were included during the June 1st release. Both vulnerabilities are the type that are usually leveraged by malware that has sneaked into a device through a low-privilege pathway such as a threat actor installing a seemingly harmless application to raise their execution or access authorization as required for nefarious activity.
The fourth critical vulnerability addressed during the June 1st patch level involves the Media Codecs component and is tracked as CVE-2022-20130 . The fifth critical vulnerability fix mentioned in the June 5th patch level involves Unisoc chips only and is tracked as CVE-2022-20210. Researchers found that this flaw makes it possible for a threat actor to neutralize a device's radio communication by using a malformed packet. It is worth mentioning that Unisoc accounts make up about 11% of the Android market and most devices are found in “affordable or rugged devices used in the military.”

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.

Apple

Apple released an update for macOS Big Sur 11.6.7. This update addresses an issue that could Mail and apps, such as Microsoft Outlook to be unable open attachments if the app required to open the file is already running. At this time, a CVE entry has not been published but the update is still significant because macOS Big Sur updates improve the compatibility, stability, as well as performance of Mac devices and are recommended for all macOS Big Sur users. 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 22 security advisories this month, three with a "Critical" severity rating and nine have a "High" severity rating. Additional information on the security advisories categorized as 'critical' is as follows:

- CVE-2022-20798 (9.8 CVSS score) - A vulnerability in the external authentication functionality of Cisco Secure Email and Web Manager, formerly known as Cisco Security Management Appliance (SMA), and Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote threat actor to bypass authentication and log in to the web management interface of an affected device.
- CVE-2022-20825 (9.8 CVSS score) - A vulnerability in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is caused by insufficient user input validation of incoming HTTP packets. A threat actor could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could give a threat actor the ability to execute arbitrary commands on an affected device using root-level privileges. At this time, Cisco has not released software updates to address this vulnerability and there are no workarounds available.
- CVE-2022-22965 (9.8 CVSS score) –This is an update to this vulnerability that was originally released in March 2022. This critical flaw involves the Spring Framework affecting Spring MVC and Spring WebFlux applications running on JDK 9+. For a complete details on this vulnerability and workarounds click here.

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 the vulnerabilities listed in their security advisory. HC3 recommends users and administrators apply necessary patches immediately.

HC3: Monthly Cybersecurity Vulnerability Bulletin
July 13, 2022 TLP: White Report: 202207131000

Adobe

Adobe released six patches addressing 46 CVEs in Adobe Illustrator, InDesign, InCopy, Bridge, Robohelp, and Animate this month. Illustrator has the largest update which addresses 17 total CVEs, the most severe of these flaws could allow code execution if an affected system opens a specially crafted file. Many of these vulnerabilities fall into the Out-Of-Bounds (OOB) Write category. The update for Adobe Bridge fixes 12 bugs, 11 of which are rated 'Critical.' The patch for InCopy addresses eight 'Critical' rated vulnerabilities, that could possibly lead to arbitrary code execution. The InDesign patch addresses seven 'Critical' rated arbitrary code execution bugs. The vulnerabilities are a mix of OOB Read, OOB Write, heap overflow, and Use-After-Free (UAF) vulnerabilities for both InDesign and InCopy. The vulnerability fixed by the Animate patch is also a 'Critical' rated OOB Write that could lead to arbitrary code execution. The last flaw addressed was the Robohelp patch that fixes a 'Moderate' rated privilege escalation vulnerability caused by improper authorization. At this time, none of the vulnerabilities addressed by Adobe this month are listed as publicly known or under active attack. HC3 recommends applying the appropriate security updates and patches that can be found on Adobe's Product Security Incident Response Team (PSIRT) by clicking here.

Mozilla

Mozilla released security updates to address three vulnerabilities with a "High" rating in Firefox, Firefox ESR, and Thunderbird. CVE-2022-34479, CVE-2022-34470, CVE-2022-34468 are the "High" severity security vulnerabilities fixed this month and affected the following Mozilla products: MFSA2022-24: Firefox 102, MFSA 2022-25: Firefox ESR 91.11, and MFSA 2022-26 : Thunderbird 91.11 and 102. If successful a threat actor could exploit these vulnerabilities to take control of an affected system. HC3 recommends that all users review Mozilla security advisories and apply the necessary patches immediately.

Intel

Intel issued three security center advisories for their products this month. These security advisories are fixes or workarounds for vulnerabilities that are identified with Intel products. The following vulnerabilities were addressed:

- INTEL-SA-00615 (CVE-2022-21123, 6.1 CVSS score). Intel Processors MMIO Stale Data Advisory - Some Intel Processors could allow information disclosure due to possible security vulnerabilities in Memory Mapped I/O (MMIO. Intel is releasing firmware updates to mitigate this threat. (Additional vulnerabilities: CVE-2022-21125 5.6 CVSS score, CVE-2022-21127 5.5 CVSS score, CVE-2022-21166 5.5 CVSS score)
- INTEL-SA-00645(CVE-2022-21180, 5.5 CVSS score) - Intel Processors MMIO Undefined Access Advisory - Some 14nm Client/Xeon E3 Intel Processors may have a security vulnerability in Memory Mapped I/O (MMIO) that could allow a denial of service in certain virtualized environments.
- INTEL-SA-00698(CVE-2022-24436, 6.5 CVSS score). Software Developer Guidance for Power Advisory - Some Intel Processors have a security vulnerability that could allow information disclosure. Intel is releasing guidance to address this potential vulnerability.

Intel's software security guidance can be viewed by clicking here. HC3 recommends users apply necessary updates and patches immediately.

SAP

SAP has released 12 security notes or updates to address vulnerabilities affecting multiple products. If successful a threat actor could exploit some of these vulnerabilities to take control of a compromised system. The June release contained one vulnerability with severity a rating of "Hot News" which is the most severe and two vulnerabilities with a "High" severity rating. A breakdown of each is as follows:

- Hot News:

  Security Note# 2622660 (10 CVSS score) - This is an update to a security note that was released during Patch Tuesday in April of 2018. The security update was for the browser control Google Chromium delivered with SAP Business Client. Product: SAP Business Client (version 6.5). If you use this version, it is recommended that you implement this immediately.

- High:

  Security Note# 3158375 or CVE-2022-27668 (8.6 CVSS score) – Depending on the configuration of the route permission table in file 'saprouttab', it is possible for an unauthenticated threat actor to execute SAProuter administration commands in SAP NetWeaver and ABAP Platform- versions KERNEL 7.49, 7.77, 7.81, 7.85, 7.86, 7.87, 7.88, KRNL64NUC 7.49, KRNL64UC 7.49, SAP_ROUTER 7.53, 7.22, from a remote client, for example stopping the SAProuter, that could highly impact systems availability. SAP generally recommends avoiding wildcards (*) for the target host and the target port in "P" and "S" entries in the route permission table.

  Security Note# 3197005 or CVE-2022-31590 (7.8 CVSS score) - SAP PowerDesigner Proxy - version 16.7, allows a threat actor with local access and low privileges, the ability to work around system & #8217's root disk access restrictions to Write/Create a program file on system disk root path, which could then be executed with elevated privileges of the application during application start up or reboot, potentially compromising Confidentiality, Integrity and Availability of the system.

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.

References

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

Android and Google Service Mitigations
https://source.android.com/security/bulletin/2022-06-01#mitigations

Android June 2022 updates bring fix for critical RCE vulnerability
https://www.bleepingcomputer.com/news/security/android-june-2022-updates-bring-fix-for-critical-rce-vulnerability/

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

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

Global Smartphone Application Processor (AP) Market Share: By Quarter
https://www.counterpointresearch.com/global-smartphone-ap-market-share/

Intel Product Security Center Advisories
https://www.intel.com/content/www/us/en/security-center/default.html

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

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/

Microsoft to start nagging Windows 8.1 users in July about January 2023 end-of-support date
https://www.zdnet.com/article/microsoft-to-start-nagging-windows-8-1-users-in-july-about-january-2023-end-of-support-date/

Mozilla Releases Security Updates for Firefox, Firefox ESR, and Thunderbird
https://www.cisa.gov/uscert/ncas/current-activity/2022/06/29/mozilla-releases-security-updates-firefox-firefox-esr-and

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

Microsoft patches actively exploited Follina Windows zero-day
https://www.bleepingcomputer.com/news/security/microsoft-patches-actively-exploited-follina-windows-zero-day/

Microsoft Patch Tuesday, June 2022 Edition
https://krebsonsecurity.com/2022/06/microsoft-patch-tuesday-june-2022-edition/#:~:text=On%20top%20of%20the%20critical,a%20service%20built%20into%20Windows.

Microsoft June 2022 Patch Tuesday
https://isc.sans.edu/forums/diary/Microsoft+June+2022+Patch+Tuesday/28742/

Microsoft June 2022 Patch Tuesday: 55 fixes, remote code execution in abundance
https://www.zdnet.com/article/microsoft-june-2022-patch-tuesday-55-fixes-remote-code-execution-in-abundance/

Microsoft June 2022 Patch Tuesday fixes 1 zero-day, 55 flaws
https://www.bleepingcomputer.com/news/microsoft/microsoft-june-2022-patch-tuesday-fixes-1-zero-day-55-flaws/

SAP Releases June 2022 Security Updates
https://www.cisa.gov/uscert/ncas/current-activity/2022/06/14/sap-releases-june-2022-security-updates

SAP Security Patch Day - June 2022
https://dam.sap.com/mac/app/e/pdf/preview/embed/ucQrx6G?ltr=a&rc=10

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

The June 2022 Security Update Review
https://www.zerodayinitiative.com/blog/2022/6/14/the-june-2022-security-update-review

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