HC3: Monthly Cybersecurity Vulnerability Bulletin
July 9, 2024 TLP:CLEAR Report: 202407091500

June 2024 Vulnerabilities of Interest to the Health Sector

In June 2024, 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 June are from Snowflake, Microsoft, Google/Android, Apple, Mozilla, Cisco, SAP, VMWare, Adobe, Fortinet, and Atlassian. A vulnerability is given the classification of a zero-day when it is actively exploited with no fix available, or if it 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 nine 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 the vulnerabilities in this catalog, and consider prioritizing them as part of their risk mitigation plan. The full database can be found here.

Snowflake

Snowflake, a cloud computing, data-cloud organization, gained attention for a financially motivated attack where approximately 165 organizations were impacted from data theft and extortion using compromised credentials by UNC5537. According to Google: "The threat campaign conducted by UNC5537 has resulted in numerous successful compromises due to three primary factors:

1. The impacted accounts were not configured with multi-factor authentication enabled, meaning successful authentication only required a valid username and password.
2. Credentials identified in infostealer malware output were still valid, in some cases years after they were stolen, and had not been rotated or updated.
3. The impacted Snowflake customer instances did not have network allow lists in place to only allow access from trusted locations."

Technical information related to this campaign can be viewed here, and Mandiant's threat hunting guide for Snowflake can be viewed here. HC3 strongly encourages all users to review and apply any mitigations from the CISA and Snowflake's security advisory to prevent serious damage from occurring the Healthcare and Public Health sector.

Microsoft

Microsoft released or provided security updates for 54 vulnerabilities. There was one critical and one zero-day vulnerability addressed in the update, which were not reported to be exploited in attacks. Microsoft has also reported on 31 non-Microsoft CVEs in their June release notes, which impacts MITRE Corporation, GitHub, and Chrome. Additional information on the critical vulnerability and two zero-days can be found below:

- CVE-2024-30080: Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability.
- CVE-2023-50868: The Closest Encloser Proof aspect of the DNS protocol allows remote attackers to cause a denial of service via DNSSEC responses in a random subdomain attack.

For a complete list of Microsoft vulnerabilities and 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/Android released two updates in early June. The first update was released on June 01, 2024, and addressed eight vulnerabilities in the Framework, System components, and Google Play updates. All these vulnerabilities were given a high rating in severity, and according to Google: "The most severe vulnerability in this section could lead to local escalation of privilege with no additional execution privileges needed." The second part of Google/Android's security advisory was released on June 05, 2024, and it addressed updates in the Kernel, Arm, Imagination Technologies, MediaTek, and Qualcomm closed-source components. Three of these vulnerabilities were rated as critical in severity, and the remaining were rated as high. Additional information on the critical vulnerabilities from the National Vulnerability Database can be found below:

- CVE-2023-43538: Memory corruption in TZ Secure OS while Tunnel Invoke Manager initialization.
- CVE-2023-43551: Cryptographic issue while performing attach with a LTE network, a rogue base station can skip the authentication phase and immediately send the Security Mode Command.
- CVE-2023-43556: Memory corruption in Hypervisor when platform information mentioned is not aligned.

HC3 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 improves 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. The chrome browser update can be viewed here.

Apple

Apple released one security update in June, for AirPods (2nd generation and later), AirPods Pro (all models), AirPods Max, Powerbeats Pro, and Beats Fit Pro, which is correlated with CVE-2024-27867, and can allow an attacker within Bluetooth range to spoof the source device and gain access to your headphones.

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 four security advisories in June, addressing vulnerabilities affecting Thunderbird, Firefox for iOS, Firefox ESR, and Firefox. All these vulnerabilities were rated as high in severity. HC3 encourages all users to the following advisories and apply the necessary updates:

- Thunderbird 115.12
- Firefox 125
- Firefox ESR 115.12
- Firefox for iOS 127

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.

Cisco

Cisco released eight security updates to address vulnerabilities in multiple products. Three of the vulnerabilities were classified as "High" in severity, four were classified as "Medium," and the remaining one was classified as "Informational" in severity.

For a complete list of Cisco security advisories released in June, 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.

SAP

SAP released ten security notes and three updates to previously issued security notes to address vulnerabilities affecting multiple products. If successful in launching an attack, a threat actor could exploit these vulnerabilities and take control of a compromised device or system. This month, there were no reported vulnerabilities with a severity rating of "Hot News", which is the most severe and a top priority for SAP. The remaining flaws consisted of two "High", eight "Medium", and three "Low" rated vulnerabilities in severity. A breakdown of the High security notes for the month of June can be found below:

- **Security Note #3457592** (CVE-2024-37177): This vulnerability was given a CVSS score of 8.1 and is a cross-site scripting (XSS) vulnerabilities in SAP Financial Consolidation.
- **Security Note #3460407** (CVE-2024-34688): This vulnerability was given a CVSS score of 7.5 and it is a denial of service (DOS) in SAP NetWeaver AS Java.

For a complete list of SAP's security notes and updates for vulnerabilities released in June, 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 moderate security advisory update, which addresses an information exposure

vulnerability in VMware Workspace One UEM. Additional information on this vulnerability is listed below:

- OMSA-2024-0008 (CVE-2024-22260): According to VMware: "Workspace ONE UEM endpoints contain an information exposure vulnerability. VMware has evaluated the severity of this issue to be in the Moderate severity range with a maximum CVSSv3 base score of 6.8."

For a complete list of VMWare's security advisories, click here. Patches are available to remediate these vulnerabilities found in VMWare products. To remediate the listed vulnerabilities, apply the updates listed in the 'Fixed Version' column of the 'Response Matrix' below to affected deployments. HC3 recommends users follow VMWare's guidance for each, and apply patches listed in the 'Fixed Version' column of the 'Response Matrix' that can be accessed by clicking directly on the security advisory.

Adobe

For the month of June, Adobe released multiple security advisories for different products. HC3 recommends all users review the following bulletins and apply the necessary updates and patches immediately.

- Adobe Photoshop
- Adobe Experience Manager
- Adobe Audition
- Adobe Media Encoder
- Adobe FrameMaker Publishing Server
- Adobe Commerce
- Adobe ColdFusion
- Adobe Substance 3D Stager
- Adobe Creative Cloud Desktop
- Adobe Acrobat Android

Fortinet

Fortinet's June vulnerability advisories addressed five vulnerabilities. One of these vulnerabilities was rated as high in severity and impacts multiple versions of FortiOS. The vulnerability is tracked as CVE-2024-23110 and can, according to Fortinet, "allow an authenticated attacker to execute unauthorized code or commands via specially crafted command line arguments." Three of the other vulnerabilities were rated as medium in severity, and the remaining one was classified as low in severity. If successful, a threat actor can exploit these vulnerabilities and take control of a compromised device or system. HC3 recommends all users review Fortinet's Vulnerability Advisory page, and apply all necessary updates and patches immediately:

- FG-IR-24-036
- FG-IR-23-471
- FG-IR-23-460
- FG-IR-23-356

Atlassian

Atlassian released a security advisory regarding nine high-severity vulnerabilities in their June 2024 Security Bulletin. The highest vulnerability was rated as 8.2 on the CVSS scale and is tracked as CVE-2024-22257. CVE-2024-22257 is a dependency vulnerability that impacts the Bamboo Data Center and Server, and can allow an unauthenticated actor to expose assets in an environment, impacting the confidentiality of information.

For a complete list of security advisories and bulletins from Atlassian, click here. HC3 recommends all users apply necessary updates and patches immediately.

References

Adobe Security Updates
Adobe Product Security Incident Response Team (PSIRT)

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

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

Atlassian Security Bulletin
Security Advisories | Atlassian

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

Fortinet PSIRT Advisories
PSIRT Advisories | FortiGuard

Microsoft June 2024 Patch Tuesday fixes 51 security flaws, 18 RCEs
https://www.bleepingcomputer.com/news/microsoft/microsoft-june-2024-patch-tuesday-fixes-51-flaws-18-rces/

Microsoft June 2024 Patch Tuesday
https://isc.sans.edu/diary/Microsoft+Patch+Tuesday+June+2024/31000/

Microsoft Month Archives: June 2024
2024/06 | Microsoft Security Response Center

Mozilla Foundation Security Advisory 2024-28
Security Vulnerabilities fixed in Thunderbird 115.12 — Mozilla

Mozilla Foundation Security Advisory 2024-27
Security Vulnerabilities fixed in Firefox for iOS 127 — Mozilla
Mozilla Foundation Security Advisory 2024-26
Security Vulnerabilities fixed in Firefox ESR 115.12 — Mozilla

Mozilla Foundation Security Advisory 2024-25
Security Vulnerabilities fixed in Firefox 127 — Mozilla

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

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

SAP Security Patch Day – June 2024
https://support.sap.com/en/my-support/knowledge-base/security-notes-news/june-2024.html

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

Snowflake Recommends Customers Take Steps to Prevent Unauthorized Access
https://www.cisa.gov/news-events/alerts/2024/06/03/snowflake-recommends-customers-take-steps-prevent-unauthorized-access

Snowflake: Detecting and Preventing Unauthorized User Access: Instructions
https://community.snowflake.com/s/article/Communication-ID-0108977-Additional-Information

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