HC3: Monthly Cybersecurity Vulnerability Bulletin
September 13, 2024 TLP:CLEAR Report: 202409131200

August Vulnerabilities of Interest to the Health Sector

In August 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 August are from Microsoft, Google/Android, Apple, Mozilla, Cisco, SAP, Adobe, Fortinet, Ivanti 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 nineteen vulnerabilities in August 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.

Microsoft

Microsoft released or provided security updates for 90 vulnerabilities. There were six zero-day vulnerabilities, three of which are reported to be actively exploited, addressed in the update. Microsoft has also reported on 12 non-Microsoft CVEs in their August release notes that impact Red Hat, Inc., and Chrome. Additional information on the zero-day vulnerabilities can be found below. HC3 encourages all users to follow CISA's guidance and apply any necessary updates, as a threat actor could exploit these vulnerabilities to take control of an affected system.

- CVE-2024-38178: Scripting Engine Memory Corruption Vulnerability
- CVE-2024-38193: Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
- CVE-2024-38213: Windows Mark of the Web Security Feature Bypass Vulnerability
- CVE-2024-38106: Windows Kernel Elevation of Privilege Vulnerability
- CVE-2024-38107: Windows Power Dependency Coordinator Elevation of Privilege Vulnerability
- CVE-2024-38189: Microsoft Project Remote Code Execution Vulnerability

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.

HC3: Monthly Cybersecurity Vulnerability Bulletin
September 13, 2024 TLP:CLEAR Report: 202409131200

Google/Android

Google/Android released two updates in early August. The first update was released on August 01, 2024, and addressed ten vulnerabilities in the Framework and System updates. All of these vulnerabilities were rated as high in severity, and according to Google: "The most severe of these issues could lead to local escalation of privilege with no additional execution privileges needed."

The second part of Google/Androids' security advisory was released on August 05, 2024, and it addressed updates in the Kernel, Arm, Imagination Technologies, MediaTek, Qualcomm, and Qualcomm closed-source components. One of these vulnerabilities was rated as critical, and the remaining were given a high rating in severity. Additional information on the critical vulnerabilities from the National Vulnerability Database can be found below:

- CVE-2024-23350: Permanent DOS when DL NAS transport receives multiple payloads, such that one payload contains SOR container whose integrity check has failed, and the other is LPP where UE needs to send status message to network.

Additionally, it was reported that the Qilin ransomware operator(s) had been stealing credentials stored in Google Chrome. The attack, which was analyzed by researchers from Sophos, involved compromised credentials for a VPN that was not enabled with MFA. After obtaining initial access, the attackers had a dwell period of 18 days, which was possibly used to map the network and identify critical assets, and ultimately led to the execution of ransomware.

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.

Apple

HC3 encourages users and administrators to review the following advisories and apply necessary updates, as a threat actor could exploit these vulnerabilities to take control of an affected system:

- iOS 17.6.1 and iPadOS 17.6.1
- iOS 16.7.10 and iPadOS 16.7.10
- macOS Sonoma 14.6.1
- macOS Ventura 13.6.9
- watchOS 10.6.1
- tvOS 17.6.1

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 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 follow these advisories and apply the necessary updates:

- Thunderbird 115.14
- Thunderbird 128.1
- Firefox ESR 115.14
- Firefox for iOS 129

- Firefox 129
- Firefox ESR 128.1

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 23 security updates to address vulnerabilities in multiple products. Two of these updates were rated critical, five were rated as high, and the remaining were scored as medium in severity. Additional information on the critical vulnerabilities can be found below:

- CVE-2024-20419: A vulnerability in the authentication system of Cisco Smart Software Manager On-Prem could allow an unauthenticated, remote attacker to change the password of any user, including administrative users.
- CVE-2024-20450, 20451, 20452: Multiple vulnerabilities in the web-based management interface of Cisco Small Business SPA300 Series IP Phones and Cisco Small Business SPA500 Series IP Phones could allow an attacker to execute arbitrary commands on the underlying operating system or cause a denial-of-service condition.

For a complete list of Cisco security advisories released in August, 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 17 security notes and eight 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 two 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 four "High", and nineteen "Medium" rated vulnerabilities in severity. A breakdown of the High security notes for the month of April can be found below:

- **Security Note #3479478** (CVE-2024-41730): This vulnerability was given a CVSS score of 9.8 and is a missing authorization check in SAP BusinessObjects Business Intelligence Platform.
- **Security Note #3477196** (CVE-2024-29415): This vulnerability was given a CVSS score of 9.1 and it is an Server-Side request forgery vulnerability in applications with SAP Build apps.

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

Adobe

Adobe released multiple security updates to address vulnerabilities for multiple different products. HC3 recommends all users follow CISA's guidance and review the following bulletins and apply the necessary updates and patches immediately.

- Security Update Available for Adobe Illustrator | APSB24-45
- Security Update Available for Adobe Dimension | APSB24-47
- Security Update Available for Adobe Photoshop | APSB24-49
- Security Update Available for Adobe InDesign | APSB24-56
- Security Update Available for Adobe Acrobat Reader | APSB24-57
- Security Update Available for Adobe Bridge | APSB24-59
- Security Update Available for Adobe Substance 3D Stager | APSB24-60
- Security Update Available for Adobe Commerce and Magneto | APSB24-61
- Security Update Available for Adobe InCopy | APSB24-64
- Security Update Available for Adobe Substance 3D Sampler | APSB24-65
- Security Update Available for Adobe Substance 3D Designer | APSB24-67

HC3 recommends applying the appropriate security updates or patches that can be found on Adobe's Product Security Incident Response Team (PSIRT) by clicking here, because an attacker could exploit some of these vulnerabilities to control of a compromised system.

Fortinet

Fortinet's August vulnerability advisories addressed three vulnerabilities. Two of these vulnerabilities were rated as medium in severity, and impacts multiple versions of FortiOS, FortiAnalyzer, and FortiManager. The remaining vulnerability was rated 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-22-445
- FG-IR-23-467
- FG-IR-24-012

Ivanti

Ivanti released security updates for Avalanche, Neurons for ITSM, and Virtual Traffic Manager, which a threat actor could exploit to take control of. HC3 encourages all users to review the advisories and follow CISA's guidance and apply any necessary updates:

- Security Advisory: Ivanti Avalanche
- Security Advisory: Ivanti Neurons for ITSM
- Security Advisory: Ivanti Virtual Traffic Manager (vTM)

Atlassian

Atlassian released a security advisory regarding nine high-severity vulnerabilities in their August 2024 Security Bulletin. The highest vulnerabilities are rated 8.1 on the CVSS scale and are tracked as CVE-2024-22259, CVE-2024-22243, and CVE-2024-22262. All three of these vulnerabilities impact the Crowd Data Center and Server and are a Server-Side Forgery Dependency vulnerability, which can allow an unauthenticated attacker to expose assets in the environment, without requiring user interaction.

A complete list of security advisories and bulletins from Atlassian can be viewed 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

Qilin ransomware caught stealing credentials stored in Google Chrome
https://news.sophos.com/en-us/2024/08/22/qilin-ransomware-caught-stealing-credentials-stored-in-google-chrome/

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

Microsoft August 2024 Patch Tuesday fixes 9 zero-days, 6 exploited
https://www.bleepingcomputer.com/news/security/qilin-ransomware-now-steals-credentials-from-chrome-browsers/

Microsoft August 2024 Patch Tuesday
https://isc.sans.edu/diary/Microsoft+August+2023+Patch+Tuesday/30106

Microsoft Month Archives: August 2024
2024/08 | Microsoft Security Response Center

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

SAP Security Patch Day – August 2024
SAP Security Patch Day – August 2024

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

VMware Security Advisories
https://support.broadcom.com/web/ecx/security-advisory

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