HC3: Monthly Cybersecurity Vulnerability Bulletin
April 10, 2024 TLP:CLEAR Report: 202404101500

March Vulnerabilities of Interest to the Health Sector

In March 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 March are from Ivanti, 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 10 vulnerabilities in March 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 that 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.

Ivanti

Ivanti released security updates regarding the Ivanti Standalone Sentry and Ivanti Neurons for ITSM. Both vulnerabilities were rated as critical in severity. The Standalone Sentry vulnerability impacts versions 9.17.0, 9.18.0, and 9.19.0. According to Ivanti, older versions are also at risk. The vulnerability is tracked as CVE-2023-41724 and can allow an unauthenticated threat actor to execute arbitrary commands on the underlying operating system of the appliance. The second vulnerability is tracked as CVE-2023-46808 and is described as allowing an authenticated remote attacker to perform files writes to the ITSM server. Ivanti stated in their bulletin that "the patch has been applied to all Ivanti Neurons for ITSM Cloud landscapes. No further action is needed for cloud customers."

HC3 is currently unaware of either of these vulnerabilities being exploited in the wild, but strongly encourages all users to apply any necessary updates or mitigations to prevent serious damage from occurring to the HPH sector.

Microsoft

Microsoft released or provided security updates for 61 vulnerabilities. There were no zero-day vulnerabilities addressed in the updates. Two of these vulnerabilities were rated as critical in severity. Microsoft has also reported on four non-Microsoft CVEs in their March release notes that impact Chrome.

Additional information on the critical vulnerabilities from the national vulnerability database can be found below:

- CVE-2024-21334: Open Management Infrastructure (OMI) Remote Code Execution Vulnerability
- CVE-2024-21400: Microsoft Azure Kubernetes Service Confidential Container Remote Code Execution Vulnerability

For a complete list of Microsoft vulnerabilities and security updates, click here. HC3 recommends that 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 March. The first update was released on March 01, 2024 and addressed thirteen vulnerabilities in the Framework and System components. Two of these vulnerabilities were given a critical rating and the remaining were rated as high in severity. According to Google: "The most severe vulnerability in this section could lead to remote code execution with no additional execution privileges needed." The critical vulnerabilities are tracked as CVE-2024-0039 and CVE-2024-23717. They both impact version 11, 12, 12L, 13, and 14 of Android. The second part of Google/Androids' security advisory was released on March 05, 2024, and it addressed updates in the AMLogic, Arm, MediaTek, Qualcomm components, and Qualcomm closed-source components. One of these vulnerabilities was rated as critical in severity, and the remaining were rated as high. Additional information on the critical vulnerability can be found below:

- CVE-2023-28578: Memory corruption in Core Services while executing the command for removing a single event listener.

HC3 recommends that 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

Apple released multiple security updates in March, for several different products. HC3 recommends following CISA's guidance, which encourages users and administrators to review the following alerts and apply any necessary updates:

- iOS 17.7 and iPadOS 17.4
- iOS 16.7.6 and iPadOS 16.7.6
- Safari 17.4
- macOS Sonoma 14.4
- macOS Ventura 13.6.5
- macOS Monterey 12.7.4
- watchOS 10.4
- tvOS 17.4
- visionOS 1.1
- Safari 17.4.1
- macOS Sonoma 14.4.1
- macOS Ventura 13.6.6

For a complete list of the latest Apple security and software updates, click here. HC3 recommends that 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 in March addressing vulnerabilities affecting Firefox, Firefox ESR, and Thunderbird. Mozilla Firefox version 124.0.1 has been identified to be affected by two critical vulnerabilities, tracked as CVE-2024-29943 and CVE-2024-29944. CVE-2024-29943 represents a security flaw that can allow an attacker to perform an out-of-bounds read or write on a JavaScript object. CVE-2024-29944 can allow an attacker to inject an event handler into a privileged object, which would allow arbitrary JavaScript execution in the parent process. Firefox ESR version 115.9.1 is also impacted by CVE-2024-29944. HC3 encourages all users to review the following advisories and apply the necessary updates:

- Thunderbird 115.8.1
- Firefox 124
- Firefox ESR 115.9
- Firefox 124.0.1
- Firefox ESR 115.9.1
- Thunderbird 115.9

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 35 security updates to address vulnerabilities in multiple products. One of the vulnerabilities was classified as "Critical" in severity, and 16 were classified as "High," while the remaining were classified as "Medium" in severity. The critical vulnerability impacts Cisco SD-WAN vManage software (CVE-2023-20214). According to Cisco, this vulnerability "could allow an unauthenticated, remote attacker to gain read permissions or limited write permissions to the configuration of an affected Cisco SD-WAN vManage instance". Additionally, CISA released several security advisories on Cisco products and reported that "a threat actor could exploit this vulnerability to take control of an affected system." HC3 encourages all users to review the following CISA advisories and apply the necessary updates:

- Cisco NX-OS Software
- Cisco Releases Security Updates for Secure Client
- Cisco Releases Security Updates for IOS XR Software
- Cisco Releases Security Updates for Multiple Products

For a complete list of Cisco security advisories released in March, 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 10 security notes and two 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 three

vulnerabilities with a severity rating of "Hot News", which is the most severe and a top priority for SAP. The remaining flaws consisted of three "High", and six "Medium" rated vulnerabilities in severity. A breakdown of the Hot News security notes for the month of March can be found below:

- **Security Note #2622660** (No associated CVE): This is an update to security note released on April 2018 for the browser control Google Chromium delivered with SAP Business Client.
- **Security Note #3425274** (CVE-2019-10744): This vulnerability was given a CVSS score of 9.4 and it is code injection vulnerability in SAP builds apps affecting versions 4.9.145.
- **Security Note #3433192** (CVE-2024-22127): This vulnerability was given a CVSS score of 9.1 and it is a code injection vulnerability in SAP NetWeaver AS Java affecting version 7.50.

For a complete list of SAP's security notes and updates for vulnerabilities released in March, click here. HC3 recommends patching immediately and following SAP's guidance for additional support. To fix vulnerabilities discovered in SAP products, SAP recommends that customers visit the Support Portal and apply patches to protect their SAP landscape.

VMWare

VMWare released one critical security advisory update, which addresses multiple vulnerabilities in VMware ESXi, VMware Workstation Pro /Player (Workstation), VMware Fusion Pro / Fusion, and VMware Cloud Foundation. Additional information on this vulnerability is listed below:

- VMSA-2024-0006.1 (CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, CVE-2024-22255): According to VMware: "A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. On ESXi, the exploitation is contained within the VMX sandbox whereas, on Workstation and Fusion, this may lead to code execution on the machine where Workstation or Fusion is installed."

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 that users follow VMWare's guidance for each and apply patches listed in the 'Fixed Version' column of the 'Response Matrix', which can be accessed by clicking directly on the security advisory.

Adobe

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

- Adobe Experience Manager
- Adobe Premiere Pro
- Adobe ColdFusion
- Adobe Bridge
- Adobe Lightroom
- Adobe Animate

Fortinet

Fortinet's March vulnerability advisories addressed three vulnerabilities. One of these vulnerabilities was rated as critical in severity and impacts FortiOS and FortiProxy. The vulnerabilities are tracked as CVE-

2023-42789 and CVE-2023-42790 and can result in the execution of unauthorized code or commands. According to Fortinet: "An out-of-bounds write vulnerability [CWE-787] and a Stack-based Buffer Overflow [CWE-121] in FortiOS & FortiProxy captive portal may allow an inside attacker who has access to captive portal to execute arbitrary code or commands via specially crafted HTTP requests." If successful, a threat actor can exploit this vulnerability and take control of a compromised device or system. HC3 recommends that all users review Fortinet's Vulnerability Advisory page, and apply all necessary updates and patches immediately:

- FG-IR-23-328
- FG-IR-24-013
- FG-IR-23-424

Atlassian

Atlassian released a security advisory regarding 24 high-severity vulnerabilities and 1 critical-severity vulnerability in their March 2024 Security Bulletin. The critical vulnerability was rated as 10.0 on the CVSS scale is tracked as CVE-2024-1597. CVE-2024-1597 can allow an attacker to inject SQL queries on a vulnerable system. Atlassian stated in their bulletin: "Bamboo & Other Atlassian Data Center products are unaffected by this vulnerability as they do not use the PreferQueryMode=SIMPLE in their SQL database connection settings."

A complete list of security advisories and bulletins from Atlassian can be viewed here. HC3 recommends that 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

SA: CVE-2023-46808 (Authenticated Remote File Write) for Ivanti Neurons for ITSM
https://forums.ivanti.com/s/article/SA-CVE-2023-46808-Authenticated-Remote-File-Write-for-Ivanti-Neurons-for-ITSM?language=en_US

CVE-2023-41724 (Remote Code Execution) for Ivanti Standalone Sentry
https://forums.ivanti.com/s/article/CVE-2023-41724-Remote-Code-Execution-for-Ivanti-Standalone-Sentry?language=en_US

Microsoft March 2024 Patch Tuesday fixes 60 flaws, 18 RCE bugs
https://www.bleepingcomputer.com/news/microsoft/microsoft-march-2024-patch-tuesday-fixes-60-flaws-18-rce-bugs/

Microsoft March 2024 Patch Tuesday
Microsoft Patch Tuesday - March 2024 - SANS Internet Storm Center

Microsoft Month Archives: March 2024
2024/03 | Microsoft Security Response Center

Mozilla Foundation Security Advisory 2024-16
https://www.mozilla.org/en-US/security/advisories/mfsa2024-16/

Mozilla Foundation Security Advisory 2024-15
https://www.mozilla.org/en-US/security/advisories/mfsa2024-15/

Mozilla Foundation Security Advisory 2024-14
https://www.mozilla.org/en-US/security/advisories/mfsa2024-14/

Mozilla Foundation Security Advisory 2024-13
https://www.mozilla.org/en-US/security/advisories/mfsa2024-13/

Mozilla Foundation Security Advisory 2024-12
https://www.mozilla.org/en-US/security/advisories/mfsa2024-12/

Mozilla Foundation Security Advisory 2024-11
https://www.mozilla.org/en-US/security/advisories/mfsa2024-11/

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 – March 2024
https://support.sap.com/en/my-support/knowledge-base/security-notes-news/march-2024.html

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