Office of
Information Security
Securing One HHS

Health Sector Cybersecurity
Coordination Center

HC3: Monthly Cybersecurity Vulnerability Bulletin

May 15, 2024 TLP:CLEAR Report: 202405151500

April Vulnerabilities of Interest to the Health Sector

In April 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 April are from Palo Alto, 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 given 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 April 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.

Palo Alto

Palo Alto released an advisory for a maximum severity vulnerability tracked as CVE-2024-3400. Palo Alto Networks report that this vulnerability only affects PAN-OS 10.2, PAN-OS 11.0, and PAN-OS 11.1 firewalls configured with GlobalProtect gateway or GlobalProtect portal (or both). Importantly, this issue does not impact cloud firewalls (Cloud NGFW), Panorama appliances, or Prisma Access.

The most recent update noted that they were aware of an increasing number of attacks targeting CVE-2024-3400, and the proof of concept was publicly disclosed. Reports from Unit 42 show that threat actors are using this vulnerability to set up a backdoor to leverage the access gained to move through target organizations' networks. Additionally, reports from ShadowServer show that approximately 156,000 instances have been seen daily. Palo Alto is monitoring this vulnerability under the name Operation MidnightEclipse. For further information regarding the details of this attack, including indicators of compromise, please refer to this link. Additional information on the vulnerability from Volexity can be found here. For the most up-to-date security information, we recommend accessing Palo Alto's Security Advisory.

Ivanti

Ivanti released a security advisory in April which impacts all supported versions (9.x and 22.x) of Ivanti Connect Secure and Policy Secure gateways. The vulnerabilities are tracked as CVE-2024-21894 (Heap Overflow), CVE-2024-22052 (Null Pointer Dereference), CVE-2024-22053 (Heap Overflow), CVE-2024-22023 (XML entity expansion or XXE) and CVE-2024-29205 for Ivanti Connect Secure and Ivanti Policy Secure Gateways. Ivanti is aware of a limited number of customers who have been impacted by this vulnerability. HC3 encourages users to follow CISA guidance and review the advisory, and apply any necessary updates.

Microsoft

Microsoft released or provided security updates for 149 vulnerabilities. There were two zero-day vulnerabilities addressed in the updates that were previously exploited in attacks. One of these vulnerabilities was rated as critical in severity. Microsoft has also reported on six non-Microsoft CVEs in their April release notes, which impact Intel Corporation, Lenovo, and Chrome. Additional information on the critical vulnerability and two zero-days can be found below:

- CVE-2024-26234: Proxy Driver Spoofing Vulnerability
- CVE-2024-29988: SmartScreen Prompt Security Feature Bypass Vulnerability
- CVE-2024-29990: Microsoft Azure Kubernetes Service Confidential Container Elevation of Privilege Vulnerability

For a complete list of Microsoft vulnerabilities and security updates, click here. HC3 recommends all users follow Microsoft's guidance 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 April. The first update was released on April 01, 2024, and addressed eight vulnerabilities in the Framework and System components. 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/Androids' security advisory was released on April 05, 2024, and it addressed updates in the MediaTek, Widevine, Qualcomm components, and Qualcomm closed-source components. One of these vulnerabilities was rated as critical in severity, and the remaining were rated as high in severity. Additional information on the critical vulnerability can be found below:

- CVE-2023-28582: Memory corruption in Data Modem while verifying hello-verify message during the DTLS handshake.

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. All Android and Google service mitigations, along with security information on vulnerabilities for the month of April, can be viewed here.

Apple

Apple released one security update in April, impacting visionOS 1.1.2, which has no published CVE.

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 in April addressing vulnerabilities affecting Firefox, Firefox ESR, Firefox for iOS, and Thunderbird. Three of these vulnerabilities were rated as high in severity, and one was rated as moderate. HC3 encourages all users to review the following advisories and apply the necessary updates:

- Thunderbird 115.10
- Firefox 125
- Firefox ESR 115.10
- Firefox for iOS 124

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 21 security updates to address vulnerabilities in multiple products. Six of the vulnerabilities were classified as "High" in severity, 16 as "High," and the remaining were classified as "Medium" in severity. The critical vulnerability impacts Cisco SD-WAN vManage software (CVE-2023-20214). Cisco also released security advisories reporting on the active exploitation of CVE-2024-20353 and CVE-2024-20359, which impacts Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software. Additionally, Cisco has reported on a large number of brute force attacks targeting Virtual Private Networks, web application authentication interfaces, and SSH services. HC3 also encourages all users to review the following CISA advisories and apply the necessary updates:

- Cisco Releases Security Advisories for Cisco Integrated Management Controller
- Cisco Releases Security Updates Addressing ArcaneDoor, Vulnerabilities in Cisco Firewall Platforms

For a complete list of Cisco security advisories released in April, 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. 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 three "High", and nine "Medium" rated vulnerabilities in severity. A breakdown of the High security notes for the month of April can be found below:

- **Security Note #3424839** (CVE-2024-27899): This vulnerability was given a CVSS score of 8.8 and is a security misconfiguration in SAP NetWeaver AS Java User Management Engine.
- **Security Note #3421384** (CVE-2024-25646): This vulnerability was given a CVSS score of 7.7 and it is an information disclosure vulnerability in the SAP BusinessObjects Web Intelligence product.
- **Security Note #3438234** (CVE-2024-27901): This vulnerability was given a CVSS score of 7.2 and it is a directory traversal vulnerability in SAP Asset Accounting.

For a complete list of SAP's security notes and updates for vulnerabilities released in April, 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 important security advisory update that addresses multiple vulnerabilities in VMware SD-WAN Edge and VMware SD-WAN Orchestrator. Additional information on this vulnerability is listed below:

- VMSA-2024-0008 (CVE-2024-22246, CVE-2024-2224, CVE-2024-22248): According to VMware: "VMware SD-WAN Edge contains an unauthenticated command injection vulnerability potentially leading to remote code execution. VMware has evaluated the severity of this issue to be in the important severity range with a maximum CVSSv3 base score of 7.4."

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', which can be accessed by clicking directly on the security advisory.

Adobe

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

- Adobe After Effects
- Adobe Photoshop
- Adobe Commerce and Magento
- Adobe InDesign
- Adobe Experience Manager
- Adobe Media Encode
- Adobe Bridge
- Adobe Illustrator
- Adobe Animate

Fortinet

Fortinet's April vulnerability advisories addressed three vulnerabilities. One of these vulnerabilities was rated as high in severity and impacts multiple versions of FortiOS and FortiProxy. The vulnerabilities are tracked as CVE-2023-41677, and according to Fortinet, "may allow an attacker to obtain the administrator cookie in rare and specific conditions, via tricking the administrator into visiting a malicious attacker-controlled website through the SSL-VPN." The remaining vulnerabilities were rated as medium 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-23-493
- FG-IR-23-413
- FG-IR-23-224

Atlassian

Atlassian released a security advisory regarding 7 high-severity vulnerabilities in their April 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

SA:CVE-2024-21894 (Heap Overflow), CVE-2024-22052 (Null Pointer Dereference), CVE-2024-22053 (Heap Overflow), CVE-2024-22023 (XML entity expansion or XXE) and CVE-2024-29205 for Ivanti Connect Secure and Ivanti Policy Secure Gateways
https://forums.ivanti.com/s/article/SA-CVE-2024-21894-Heap-Overflow-CVE-2024-22052-Null-Pointer-Dereference-CVE-2024-22053-Heap-Overflow-and-CVE-2024-22023-XML-entity-expansion-or-XXE-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US

Microsoft April 2024 Patch Tuesday fixes 150 security flaws, 67 RCEs
https://www.bleepingcomputer.com/news/microsoft/microsoft-april-2024-patch-tuesday-fixes-150-security-flaws-67-rces/

Microsoft April 2024 Patch Tuesday
https://isc.sans.edu/diary/April+2024+Microsoft+Patch+Tuesday+Summary/30822/

Microsoft Month Archives: April 2024
2024/04 | Microsoft Security Response Center

Mozilla Foundation Security Advisory 2024-20

Security Vulnerabilities fixed in Thunderbird 115.10 — Mozilla

Mozilla Foundation Security Advisory 2024-19
Security Vulnerabilities fixed in Firefox ESR 115.10 — Mozilla

Mozilla Foundation Security Advisory 2024-18
Security Vulnerabilities fixed in Firefox 125 — Mozilla

Mozilla Foundation Security Advisory 2024-17
Security Vulnerabilities fixed in Firefox for iOS 124 — 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 – April 2024
https://support.sap.com/en/my-support/knowledge-base/security-notes-news/april-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