HC3: Monthly Cybersecurity Vulnerability Bulletin

April 5, 2022 TLP: White Report: 202204051500

March Vulnerabilities of Interest to the Health Sector

Executive Summary

In March 2022, vulnerabilities in common information systems relevant 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, Adobe, Android, Google, Apple, Intel, Mozilla, SAP, Sophos, SonicWall, and VMWare. HC3 recommends patching all vulnerabilities with special consideration to each vulnerability criticality category against the risk management posture of the organization. As always, accountability, proper inventory management and device hygiene along with and asset tracking are imperative to an effective patch management program.

Importance to HPH Sector

DEPARTMENT OF HOMELAND SECURITY/CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

In March, the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) added 22 vulnerabilities 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 US federal enterprise. Vulnerabilities that are entered into this catalog are required to be patched by their associated deadline by all US 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

For the month of March, Microsoft released patches for 92 vulnerabilities. Three of the CVEs addressed this month are classified as Important zero-days and cover a broad range of Microsoft products. They are as follows:

- CVE-2022-21990: Remote Desktop Client remote code execution (RCE) vulnerability. This client-side vulnerability should not impact organizations as much as a server-side RDP vulnerability, but it's listing as publicly known warrants attention for SecOps teams, and it should be patched promptly. This CVE has the highest CVSS score (8.8) out of this month's three publicly known flaws. In the case of a Remote Desktop connection, an attacker with control of a Remote Desktop Server could trigger a RCE attack on the RDP client machine when a victim connects to the attacking server with the vulnerable Remote Desktop Client.
- CVE-2022-24512: .NET and Visual Studio remote code execution vulnerability. Rated as Important with a CVSS of 6.3, this vulnerability does not require any type of privileges to be exploited; however, successful exploitation of this vulnerability requires user interaction — in this case, a user triggering the payload in the application.
- CVE-2022-24459: Windows Fax and Scan Service elevation of privilege vulnerability. This affects all versions of Microsoft Server and Windows 10 and does not require user interaction or privileges. Because this has a CVSS score of 7.8 and a proof-of-concept exploit code is available, CrowdStrike recommends careful consideration of this vulnerability.

There were also three critical vulnerabilities addressed this month and according to Microsoft one is already being exploited. Information on the critical flaws for March are as follows:

- CVE-2022-23277 (CVSS 8.8) – This is a Microsoft Exchange Server Remote Code Execution vulnerability.
- CVE-2022-22006 (CVSS 7.8) - HEVC Video Extensions Remote Code Execution Vulnerability.
- CVE-2022-24501 (CVSS 7.8) - VP9 Video Extensions Remote Code Execution Vulnerability.

With CVE-2022-23277, a threat actor that has been designated an authenticated user, could attempt to trigger malicious code in the context of the server's account through a network call. For both CVE-2022-22006 and CVE-2022-24501, an threat actor could exploit the vulnerability by convincing a victim to download and open a specific file that compromise the system and cause it to crash. To view the list of Microsoft vulnerabilities released by in March and their rating click here. HC3 recommends patching and testing immediately as all vulnerabilities can adversely impact the healthcare industry.

ADOBE

In March Adobe released security updates to fix 6 vulnerabilities in Adobe Photoshop, Illustrator and After Effects. Illustrator is classified as critical, and it addresses a single buffer overflow that could lead to arbitrary code execution. There is one update for Photoshop that fixes a single Important-rated memory leak. For After Effects, there are patches for four Critical-rated, stacked-based buffer overflows that could result in arbitrary code execution. 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.

ANDROID / GOOGLE

For the month of March, Google announced that Android security updates included patches for a total of 39 vulnerabilities. The first part of the update, released March 1st, addresses CVE-2021-39708 and 17 other security flaws. The breakdown of this is as follows: There were 10 security issues resolved in the System component (nine elevation of privilege along with one information disclosure vulnerability), six flaws resolved in Framework (four elevation of privilege and two denial of service bugs), one in Media Framework (information disclosure) and one elevation of privilege was patched in Android runtime. On March 5th the second part of security updates were released and addressed 21 vulnerabilities. The second patch level includes everything in the first patch level, and it has fixes for third-party closed source and Kernel components that may not apply to all devices. It is important to note that if you are using anything than Android 10, consider an upgrade to a new and actively supported device or flashing your existing with a third-party Android ROM that's based on a recent AOSP version. In addition to this, there were two Google Play system updates for vulnerabilities in media codecs and permission controller component. Google Pixel devices with a patch level of *March 5, 2022* or later addresses all these vulnerabilities along with 41 other security holes that affect Kernel components (13 flaws), Pixel (26), Qualcomm components (1) and Qualcomm closed-source components (1).

Google also released an emergency update this month to patch a high-severity zero-day vulnerability (CVE-2022-1096)in Chrome that at the time was listed actively exploited in the wild. This flaw is a type confusion vulnerability in the V8 JavaScript engine and that could allow a threat actor to perform out-of-bounds memory access. 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 has released 87 security updates for Patch Tuesday this month for multiple vulnerabilities discovered across all Apple products and platforms including patches for that included patches for macOS Monterey 12.3, iOS 15.4 and iPadOS 15.4. If these flaws are exploited, it could allow a threat actor to execute arbitrary code on an affected device. In addition to this, Apple rolled out emergency patches March 31st to address two zero-day vulnerabilities in its mobile and desktop operating systems that the company said may have been exploited in the wild. The issues have been fixed as a part of the updates to iOS and iPadOS 15.4.1, macOS Monterey 12.3.1, tvOS 15.4.1, and watchOS 8.5.1. The vulnerability tracked as CVE-2022-22675 was anonymously reported to apply and is described by experts as an out-of-bounds write vulnerability in an audio and video decoding component called AppleAVD. If exploited AppleAVD could allow an application to execute arbitrary code with kernel privileges. According to Apple, the defect was resolved with improved bounds checking, adding it's aware that "this issue may have been actively exploited." For a complete list of the latest Apple security and software updates click here. HC3 recommends installing updates and applying patches immediately to prevent potential attacks According to Apple, after a software update is installed for iOS, iPadOS, tvOS, and watchOS, it cannot be downgraded to the previous version.

INTEL

Intel released several security advisories for the month of March. The Intel Quartus Advisory (INTEL-SA-00632) is a security advisory of note this month with a High severity rating. A few vulnerabilities related to INTEL-SA-00632 with a classification of High in severity are as follows:

- CVE-2022-21203 involves improper permissions in the SafeNet Sentinel driver for Intel(R) Quartus(R) Prime Standard Edition before version 21.1 may allow an authenticated user to potentially enable escalation of privilege via local access. The vulnerability has a High CVSS base score of 8.8.
- CVE-2021-44454 involves improper input validation in a third-party component for Intel(R) Quartus(R) Prime Pro Edition before version 21.3 may allow an authenticated user to potentially enable escalation of privilege via local access. The vulnerability has a High CVSS base score of 7.3.

For a complete list of Intel's security advisories and their vulnerabilities for March click here. With the INTEL-SA-00632 security advisory, the potential security vulnerabilities in Intel Quartus Prime Pro and Standard Editions could allow escalation of privilege, denial of service, or information disclosure. HC3 recommends following Intel's guidance which is updating Intel Quartus Prime Pro to version 21.3 or later and Intel Quartus Prime Standard Edition to version 21.1 or later. Intel has updates available for download and you can access this by clicking here. A complete list of security advisories can be accessed on Intel's Product Security Center Advisories page.

MOZILLA

HC3: Monthly Cybersecurity Vulnerability Bulletin

April 5, 2022 TLP: White Report: 202204051500

Mozilla has released security updates to address vulnerabilities in Firefox, Firefox ESR, and Thunderbird. If successful, a threat actor could exploit some of these vulnerabilities to take control of an affected system. . The following high severity vulnerabilities were found in Firefox 98, Firefox ESR 91.7, and Thunderbird 91.7 : CVE-2022-26383: (Browser window spoof using fullscreen mode), CVE-2022-26384: iframe allow-scripts sandbox bypass, CVE-2022-26387: Time-of-check time-of-use bug when verifying add-on signatures, and CVE-2022-26381: Use-after-free in text reflows. HC3 recommends that all users, review Mozilla security advisories and apply the necessary patches immediately.

SAP

For March's Patch Tuesday, SAP published a total of 12 security notes, 4 were classified as Hot News (CVSS 9.1 – 10) and1 High Priority (CVSS 7.1-8.7). Some vulnerabilities of note are as follows:

- CVE-2022-22536 (Security Note: 3123396, CVSS: 10) – This is an update to a security note released in February 2022. With this security flaw, SAP NetWeaver Application Server Java, SAP NetWeaver Application Server ABAP, ABAP Platform, SAP Content Server 7.53 and SAP Web Dispatcher are vulnerable for request smuggling and request concatenation. An unauthenticated threat actor can use arbitrary data to prepend a victim's request. This would allow the threat actor to execute functions impersonating the victim or poison intermediary Web caches. If successful, an attack could lead to complete compromise of Confidentiality, Integrity and Availability of the system.
- CVE-2021-44228 (Security Notes: 3131047, 3154684,3145987, all CVSS: 10) – This is an update to a security note released in December 2021. With this vulnerability, Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases2.3.1, 2.12.2, and 2.12.3) JNDI features used in configuration, log messages, and parameters are not able to protect against attacker-controlled LDAP and other JNDI related endpoints. This vulnerability is specific to log4j-core. If a threat actor is able to successfully control log messages or log message parameters, then the threat can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed.

For a complete list of SAP's patch day vulnerabilities click here. HC3 recommends patching immediately and following SAP's guidance for additional support. To fix vulnerabilities discovered in SAP products, SAP recommends customer visit the Support Portal and apply patches protect their SAP landscape.

SOPHOS

For Patch Tuesday, Sophos has fixed a critical vulnerability tracked CVE-2022-1040 with a 9.8 CVSS score. This flaw allows a remote threat actor, who can access the Firewall's User Portal or Webadmin interface, to bypass authentication and execute arbitrary code in Sophos Firewall versions v18.5 MR3 and older. According to Sophos, by default the hotfix released should automatically address the vulnerability however older versions and end of life models may require action manually. HC3 recommends users to follow Sophos' device access guidance by clicking here and as always applying hot fixes or patches immediately.

SonicWall

This month, SonicWall has fixed a critical vulnerability in the SonicOS security operating system that allows denial of service (DoS) attacks and could lead to remote code execution (RCE). The security flaw has a CVSS severity score of 9.4 and is a stack-based buffer over weakness that impacts multiple SonicWall

firewalls. This vulnerability is tracked as CVE-2022-22274 affects Network Security Virtual (NSv series) firewalls designed to secure the cloud, Network Security services platform (NSsp) high-end firewalls, and TZ Series entry-level desktop form factor next-generation firewalls (NGFW) for small- and medium-sized businesses (SMBs). If successful, a remote unauthenticated attacker can exploit the vulnerability by HTTP requests in low complexity attacks that don't require user interaction that could cause Denial of Service (DoS) or lead to code execution in the firewall. At this time there have been no public reports of a proof-of-concept (PoC) exploits and SonicWall has not received any reports of malicious use of this vulnerability. A list of SonicWall's affected products can be viewed by clicking here. HC3 recommends users to apply all patched and updates immediately and follow SonicWall PSIRT's guidance listed in the workaround section.

VMWARE

VMWare released total of 4 security advisories for the month of March, with 1 classified as Critical and 1 as Important.

- VMSA-2022-0008 has a maximum CVSSv3 base score of 9.1. This Critical security advisory is for the VMware Carbon Black App Control(AppC) which contains OS command injection vulnerabilities CVE-2022-22951 and CVE-2022-22952. If successful, an authenticated, high privileged malicious actor with network access to the VMware App Control administration interface may be able to execute commands on the server due to improper input validation leading to remote code execution. Fixes for CVE-2022-22951 can be found in apply the patches listed in the 'Fixed Version' column of the 'Response Matrix' by clicking here.
- VMSA-2022-0005.1 has a maximum CVSSv3 base score of 8.8 and this high severity advisory impacts VMware NSX Data Center for vSphere (NSX-V) and VMware Cloud Foundation (Cloud Foundation). VMware NSX Data Center for vSphere contains a CLI shell injection vulnerability (CVE-2022-22945)in the NSX Edge appliance component. A threat actor that is able to gain SSH access to an NSX-Edge appliance (NSX-V) can execute arbitrary commands on the operating system as root. Workarounds and fixes for CVE-2022-22945can be found in the 'Fixed Version' column of the 'Response Matrix' by clicking here.

HC3 recommends that VMWare users to check for frequent updates, keep software update, and to apply patches immediately. For a complete list of this month's VMWare Security advisories click here.

Recently Published Information

Android Security Bulletin-March 2022
https://source.android.com/security/bulletin/2022-03-01

Android's March 2022 Security Updates Patch 39 Vulnerabilities
https://www.securityweek.com/androids-march-2022-security-updates-patch-39-vulnerabilities

Apple Issues Patches for 2 Actively Exploited Zero-Days in iPhone, iPad and Mac Devices
https://thehackernews.com/2022/03/apple-issues-patches-for-2-actively.html

Apple patches 87 security holes – from iPhones and Macs to Windows
https://nakedsecurity.sophos.com/2022/03/15/apple-patches-87-security-holes-from-iphones-and-macs-to-windows/

Apple Releases Security Updates for Multiple Products
https://www.cisa.gov/uscert/ncas/current-activity/2022/03/16/apple-releases-security-updates-multiple-products

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

Drupal Releases Security Updates
https://www.cisa.gov/uscert/ncas/current-activity/2022/03/17/drupal-releases-security-updates

Critical Sophos Firewall vulnerability allows remote code execution
https://www.bleepingcomputer.com/news/security/critical-sophos-firewall-vulnerability-allows-remote-code-execution/

Critical SonicWall firewall patch not released for all devices
https://www.bleepingcomputer.com/news/security/critical-sonicwall-firewall-patch-not-released-for-all-devices/

Google Issues Urgent Chrome Update to Patch Actively Exploited Zero-Day Vulnerability
https://thehackernews.com/2022/03/google-issues-urgent-chrome-update-to.html

Google Releases Security Updates for Chrome
https://www.cisa.gov/uscert/ncas/current-activity/2022/03/28/google-releases-security-updates-chrome

ISC Releases Security Advisories for BIND
https://www.cisa.gov/uscert/ncas/current-activity/2022/03/17/isc-releases-security-advisories-bind

March 2022 Security Updates
https://msrc.microsoft.com/update-guide/releaseNote/2022-Mar

Microsoft Patch Tuesday, March 2022 Edition
https://krebsonsecurity.com/2022/03/microsoft-patch-tuesday-march-2022-edition/

Microsoft March 2022 Patch Tuesday: 71 vulnerabilities fixed
https://www.zdnet.com/article/microsoft-march-2022-patch-tuesday-71-vulnerabilities-fixed/

Mozilla Releases Security Updates
https://www.cisa.gov/uscert/ncas/current-activity/2022/03/08/mozilla-releases-security-updates

Patch Tuesday – March 2022
https://www.rapid7.com/blog/post/2022/03/08/patch-tuesday-march-2022/

Pixel Update Bulletin-March 2022
https://source.android.com/security/bulletin/pixel/2022-03-01

SAP Releases March 2022 Security Updates
https://www.cisa.gov/uscert/ncas/current-activity/2022/03/08/sap-releases-march-2022-security-updates

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

SonicWall Patches Critical Vulnerability in Firewall Appliances
https://www.securityweek.com/sonicwall-patches-critical-vulnerability-firewall-appliances

VMware Releases Security Updates
https://www.cisa.gov/uscert/ncas/current-activity/2022/03/24/vmware-releases-security-updates

VMWare Security Advisories
https://www.vmware.com/security/advisories.html

Contact Information

If you have any additional questions, please contact us at HC3@hhs.gov.

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback