HC3: Monthly Cybersecurity Vulnerability Bulletin
January 19, 2023 TLP:CLEAR Report: 202301191500

December Vulnerabilities of Interest to the Health Sector

In December 2022, 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 this month are from Microsoft, Google/Android, Apple, Intel, Cisco, SAP, Citrix, VMWare, and Fortinet. A vulnerability is given the classification as a zero-day if it is actively exploited with no fix available or 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 9 vulnerabilities in December 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 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 fixes for two zero-day vulnerabilities, one of which is actively exploited, and 49 flaws. Six of the 49 vulnerabilities addressed in this month's Patch Tuesday are classified as 'Critical' as they allow remote code execution, one of the most severe types of vulnerabilities. The number of bugs in each vulnerability category is listed as follows:

- 19 Elevation of Privilege Vulnerabilities
- 2 Security Feature Bypass Vulnerabilities
- 23 Remote Code Execution Vulnerabilities
- 3 Information Disclosure Vulnerabilities
- 3 Denial of Service Vulnerabilities
- 1 Spoofing Vulnerability

The numbers above do not include twenty-five Microsoft Edge vulnerabilities fixed on December 5th.

December's Patch Tuesday also includes fixes for two zero-day vulnerabilities, one actively exploited and the other publicly disclosed. Additional information on the actively exploited and publicly disclosed zero-day vulnerability addressed this month are as follows:

- CVE-2022-44698 is a Windows SmartScreen Security Feature Bypass Vulnerability. If successful, a threat actor can create a malicious file that can evade Mark of the Web (MOTW) defenses, which according to researchers, could lead to "limited loss of integrity and availability of security features such as Protected View in Microsoft Office, which rely on MOTW tagging."
- CVE-2022-44710 is the other publicly disclosed vulnerability, which is a DirectX Graphics Kernel Elevation of Privilege Vulnerability. According to experts, "Successful exploitation of this vulnerability requires an attacker to win a race condition. An attacker who successfully exploited this vulnerability could gain SYSTEM privileges."

For a complete list of Microsoft vulnerabilities released in December and their rating, click here, and for all security updates, click here. HC3 recommends users follow Microsoft's guidance, which is to refer to Microsoft's Security Response Center and apply all necessary updates and patches immediately, as these vulnerabilities can adversely impact the health sector.

Google/Android

Google released a security update addressing four critical-severity vulnerabilities in Android, including a remote code execution flaw exploitable through Bluetooth. December's update also fixed 45 vulnerabilities for core Android components with patch level 2022-12-01. With patch level 2022-12-05, an additional 36 vulnerabilities impacting third-party components were addressed. Some critical severity vulnerabilities addressed this month are as follows:

- CVE-2022-20411 – Remote code execution flaw in Android System, impacting Android versions 10 to 13.
- CVE-2022-20472 – Remote code execution flaw in Android Framework, impacting Android versions 10 to 13.
- CVE-2022-20473 – Remote code execution flaw in Android Framework, impacting Android versions 10 to 13.
- CVE-2022-20498 – Information disclosure flaw in Android System, impacting Android versions 10 to 13.

The remaining vulnerabilities addressed were remote code execution, denial of service, elevation of privileges (EoP), and information disclosure. This month there were also 151 Pixel-specific bugs patched by Google. In addition to providing patches for Pixel devices, the December patches were available for Galaxy range and Samsung smartphones. An emergency update was issued for Google's Chrome browser, addressing its ninth zero-day vulnerability of the year. The vulnerability, tracked as CVE-2022-4262, is a high-severity type confusion issue in Chrome's V8 JavaScript engine that could allow a remote threat actor to exploit heap corruption through a crafted HTML page. Google stated they are "aware that an exploit for CVE-2022-4262 exists in the wild."

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 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. All Android and Google service mitigations along with security information security vulnerabilities affecting Android devices can be viewed by clicking here.

HC3: Monthly Cybersecurity Vulnerability Bulletin
January 19, 2023 TLP:CLEAR Report: 202301191500

Apple

Apple released security updates to address vulnerabilities in multiple products. If successful, a remote threat actor can exploit these vulnerabilities and take control of a compromised device or system. HC3 recommends all users and administrators follow CISA's guidance, which encourages users and administrators to review Apple's security updates page and apply the necessary updates for the following:

- iCloud for Windows 14.1
- iOS 15.7.2 and iPadOS 15.7.2
- iOS 16.2 and iPadOS 16.2
- macOS Big Sur 11.7.2
- macOS Monterey 12.6.2
- macOS Ventura 13.1
- Safari 16.2
- tvOS 16.2
- watchOS 9.2

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.

Intel

Intel issued two security center advisories for their products in December. These advisories provide fixes or workarounds for vulnerabilities that are identified with Intel products. The following are some of the vulnerabilities with a high severity rating that were addressed this month:

- INTEL-SA-00789 Intel Software Products Advisory for OpenSSL Vulnerabilities (CVE-2022-3786 & CVE-2022-3602) Advisory – Improper buffer restrictions in OpenSSL before version 3.0.7 for some Intel software products may allow an unauthenticated user or threat actor to potentially enable denial of service via network access. These high severity rating vulnerabilities are being tracked as CVE-2022-3602 and CVE-2022-3786 with a CVSS score of 7.5. According to Intel, product teams will be releasing remediations for OpenSSL as quickly as possible, moving to the latest version available when developing mitigations." For advisory update and additional information, review the product matrix by clicking here.

- INTEL-SA-00801 Intel Server Boards BMC Firmware Advisory – Potential security vulnerabilities in some Intel Server Board Baseboard Management Controller (BMC) firmware could allow escalation of privilege or information disclosure. Details on vulnerabilities with a high severity rating and their hyperlinks are as follows:

    - CVE-2022-40242 (CVSS 8.3 score) – Insufficiently protected credentials in some Intel(R) Server Board BMC firmware's before versions 1.11, v0027 and 4.15 may allow an unauthenticated user to potentially enable escalation of privilege via network access.
    - CVE-2022-2827 (CVSS 7.5 score) – Improper access control in some Intel(R) Server Board BMC firmware before versions 1.11, v0027 and 4.15 may allow an unauthenticated user to potentially enable information disclosure via network access.

HC3 recommends users follows Intel's guidance to update firmware for the affected Intel Server Boards to the latest version. For a complete list of these updates, click here. For a complete list of Intel's security advisories and additional guidance, click here. HC3 recommends users apply all necessary updates and patches as soon as possible.

Cisco

Cisco released security updates to address vulnerabilities in multiple products including a security advisory for a vulnerability affecting IP Phone 7800 and 8800 Series. If a remote threat actor is able to successfully exploit this vulnerability, it could cause a denial-of-service condition. HC3 recommends all users follow CISA's guidance to review the security advisory for Cisco IP Phone 7800 and 8800 Series Cisco Discovery Protocol Stack Overflow Vulnerability and apply the necessary updates.

For a complete list of Cisco security advisories released this month, 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. HC3 recommends users and administrators follow CISA's guidance and apply necessary patches immediately.

SAP

SAP released 14 new security notes and 5 updates to previously issued security notes, to address vulnerabilities affecting multiple products. If successful with launching a cyber-attack, a threat actor could exploit these vulnerabilities and take control of a compromised device or system. This month there were five vulnerabilities with severity a rating of "Hot News," which is the most severe rating. There were also five flaws classified as "High" in severity and nine as "Medium." A breakdown of some security notes for vulnerabilities with "Hot News" severity rating are as follows:

- Security Note#2622660 – has a 10.0 CVSS score and 'Hot News' severity rating. This is an update to a security note released in April 2018: Security updates for the browser control Google Chromium delivered with SAP Business Client. Product(s) impacted: SAP Business Client, Versions - 6.5, 7.0, 7.70
- Security Note#3239475 (CVE-2022-41267) – has a 9.9 CVSS score and 'Hot News' severity rating. Server-Side Request Forgery vulnerability in SAP Business Objects Business Intelligence Platform. Product(s) impacted: SAP Business Objects Business Intelligence Platform, Versions - 420, 430.
- Security Note#3273480 (CVE-2022-41272) – has a 9.9 CVSS score and 'Hot News' severity rating. Improper access control in SAP NetWeaver Process Integration (User Defined Search). Product(s) impacted: SAP NetWeaver Process Integration, Version – 7.50.
- Security Note#3271523 (CVE-2022-42889) – has a 9.8 CVSS score and 'Hot News' severity rating. Remote Code Execution vulnerability associated with Apache Commons Text in SAP Commerce. Product(s) impacted: SAP Commerce, Versions - 1905, 2005, 2105, 2011, 2205.
- Security Note#3267780 (CVE-2022-41271) – has a 9.4 CVSS score and 'Hot News' severity rating. Improper access control in SAP NetWeaver Process Integration (Messaging System). Product(s) impacted: SAP NetWeaver Process Integration, Version – 7.50.

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

Citrix

Citrix released security updates addressing a critical vulnerability, tracked as CVE-2022-27518, in Citrix ADC and Citrix Gateway. If successful, a remote threat actor could exploit one of these vulnerabilities and take control of a compromised device or system. HC3 recommends all users follows CISA's guidance, which encourages users to review the following and apply the necessary updates:

- Citrix security bulletin CTX457836
- Citrix's blog post

In addition to this, CISA is urging organizations to review the NSA's advisory APT5: Citrix ADC Threat Hunting Guidance for detection and mitigation guidance against tools employed by a malicious actor targeting vulnerable Citrix ADC systems. HC3 recommends users follows CISA's guidance and apply necessary updates or patches immediately.

VMWare

VMWare released five security advisories. Two advisories have a 'Critical' severity rating, and three have an 'Important' severity rating. Additional information on some of the severe vulnerabilities are as follows:

- VMSA-2022-0033 – This advisory has a maximum CVSSv3 base score of 9.3 and a 'Critical' severity rating. Tracked as CVE-2022-31705 , this is a heap out-of-bounds write vulnerability in the USB 2.0 controller (EHCI) of in VMware ESXi, Workstation, and Fusion. If successful, a threat actor with local administrative privileges on a virtual machine can 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, which could possibly lead to code execution on the machine where Workstation or Fusion is installed. HC3 recommends users follows VMWare's remediation guidance for this vulnerability and apply the patches listed in the 'Fixed Version' column of the 'Response Matrix' that can be accessed by clicking here.
- VMSA-2022-0031 – This advisory has a maximum CVSSv3 base score of 9.8, a 'Critical' severity rating, and is being tracked as CVE-2022-31702 and CVE-2022-31703. According to VMWare, CVE-2022-31702 vRealize Network Insight (vRNI) has a command injection vulnerability in the vRNI REST API. If a threat actor is able to gain network access to the vRNI REST API , commands without authentication can be executed. CVE-2022-31703 is a vRealize Network Insight (vRNI) directory traversal vulnerability in vRNI REST API. If a threat actor successfully gains network access to the vRNI REST API, the threat actor will have the ability to read arbitrary files from the server. HC3 recommends users follow VMWare's remediation guidance for this vulnerability and apply the patches listed in the 'Fixed Version' column of the 'Response Matrix' which can be accessed by clicking here.

For a complete list of VMWare's security advisories, click here. HC3 recommends users follow VMWare's guidance for each and immediately apply patches listed in the 'Fixed Version' column of the 'Response Matrix' that can be accessed by clicking directly on the security advisory.

Fortinet

Security provider Fortinet provided a patch to address a heap-based buffer overflow vulnerability in FortiOS SSL-VPN. This vulnerability could allow an unauthenticated remote threat actor to execute arbitrary code or commands via specifically crafted requests. This flaw, tracked as CVE-2022-42475, has already been

used in attacks and has a CVSSv3 score of 9.3. According to Fortinet, they are aware of "an instance where this vulnerability was exploited in the wild and recommends immediately validating your systems." HC3 recommends that users review FortiGuard Labs - Fortinet's PSIRT Advisories page by clicking here and apply necessary patches or updates immediately.

References

2022 Patch Tuesday cycle wraps with 48 CVEs, one advisory
https://news.sophos.com/en-us/2022/12/13/2022-patch-tuesday-cycle-wraps/

Android Security Bulletin – December 2022
https://source.android.com/docs/security/bulletin/2022-12-01

About the security content of Xcode 14.1 (Apple)
https://support.apple.com/en-us/HT213496

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

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

Cisco Releases Security Advisory for IP Phone 7800 and 8800 Series
https://www.cisa.gov/uscert/ncas/current-activity/2022/12/09/cisco-releases-security-advisory-ip-phone-7800-and-8800-series

Cisco discloses high-severity IP phone zero-day with exploit code
https://www.bleepingcomputer.com/news/security/cisco-discloses-high-severity-ip-phone-zero-day-with-exploit-code/

Citrix urges admins to patch critical ADC, Gateway auth bypass
https://www.bleepingcomputer.com/news/security/citrix-urges-admins-to-patch-critical-adc-gateway-auth-bypass/

Citrix Releases Security Updates for Citrix ADC, Citrix Gateway
https://www.cisa.gov/uscert/ncas/current-activity/2022/12/13/citrix-releases-security-updates-citrix-adc-citrix-gateway

CVE-2022-41040 and CVE-2022-41082 – zero-days in MS Exchange
https://securelist.com/cve-2022-41040-and-cve-2022-41082-zero-days-in-ms-exchange/108364/

CISA Bulletin (SB22-353) Vulnerability Summary for the Week of December 12, 2022
https://www.cisa.gov/uscert/ncas/bulletins/sb22-353

December 2022 Security Updates
https://msrc.microsoft.com/update-guide/releaseNote/2022-Dec

FortiGuard Labs - Fortinet's PSIRT Advisories
https://www.fortiguard.com/psirt/FG-IR-22-398

Google releases dev tool to list vulnerabilities in project dependencies
https://www.bleepingcomputer.com/news/security/google-releases-dev-tool-to-list-vulnerabilities-in-project-dependencies/

Government should go on offense against healthcare cyberattacks, says AHA
https://www.healthcareitnews.com/news/government-should-go-offense-against-healthcare-cyberattacks-says-aha

Hackers exploit critical Citrix ADC and Gateway zero-day, patch now
https://www.bleepingcomputer.com/news/security/hackers-exploit-critical-citrix-adc-and-gateway-zero-day-patch-now/

Intel Product Security Center Advisories
https://www.intel.com/content/www/us/en/security-center/default.html

Microsoft December 2022 Patch Tuesday
https://isc.sans.edu/diary/Microsoft%20December%202022%20Patch%20Tuesday/29336

Microsoft Patch Tuesday by Morphus Labs
https://patchtuesdaydashboard.com/

Microsoft patches Windows zero-day used to drop ransomware
https://www.bleepingcomputer.com/news/security/microsoft-patches-windows-zero-day-used-to-drop-ransomware/

Microsoft Patch Tuesday
https://cybersecurityasean.com/expert-opinions-opinion-byline/microsoft-patch-tuesday-summary

Microsoft Patch Tuesday, December 2022 Edition
https://krebsonsecurity.com/2022/12/microsoft-patch-tuesday-december-2022-edition/

Microsoft December 2022 Patch Tuesday fixes 2 zero-days, 49 flaws
https://www.bleepingcomputer.com/news/microsoft/microsoft-december-2022-patch-tuesday-fixes-2-zero-days-49-flaws/

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

SAP's December 2022 Security Updates Patch Critical Vulnerabilities
https://www.securityweek.com/saps-december-2022-security-updates-patch-critical-vulnerabilities

SAP Patches Critical Vulnerabilities in Commerce, Manufacturing Execution Products
https://www.securityweek.com/saps-december-2022-security-updates-patch-critical-vulnerabilities

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

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

Update Android Right Now to Fix a Scary Remote-Execution Flaw
https://www.wired.com/story/android-ios-16-windows-10-critical-update-december-2022/

VMware fixes critical ESXi and vRealize security flaws
https://www.bleepingcomputer.com/news/security/vmware-fixes-critical-esxi-and-vrealize-security-flaws/

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