HC3: Monthly Cybersecurity Vulnerability Bulletin
December 8, 2022 TLP:CLEAR Report: 202212081200

November Vulnerabilities of Interest to the Health Sector

In November 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, Cisco, SAP, Citrix, VMWare, OpenSSL, and Intel. 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 10 vulnerabilities in November 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

Microsoft released fixes for six actively exploited Windows vulnerabilities and a total of 68 vulnerabilities. Eleven of the 68 flaws fixed in Patch Tuesday's update are classified as 'Critical' as they allow privilege elevation, spoofing, or remote code execution, one of the most severe types of vulnerabilities. The number of bugs in each vulnerability category is listed as follows:

- 27 Elevation of Privilege Vulnerabilities
- 16 Remote Code Execution Vulnerabilities
- 11 Information Disclosure Vulnerabilities
- 4 Security Feature Bypass Vulnerabilities
- 6 Denial of Service Vulnerabilities
- 3 Spoofing Vulnerabilities

This month's Patch Tuesday also includes fixes for six actively exploited zero-day vulnerabilities; with one listed as publicly disclosed. The six actively exploited zero-day vulnerabilities fixed with this month's updates are:

- CVE-2022-41128 is a Windows Scripting Languages Remote Code Execution Vulnerability that impacts the JScript9 scripting language and could result in remote code execution. According to Microsoft, " This vulnerability requires that a user with an affected version of Windows access a

malicious server. An attacker would have no way to force users to visit this specially crafted server share or website but would have to convince them to visit the server share or website, typically by way of an enticement in an email or chat message."

- CVE-2022-41091 is a Windows Mark of the Web Security Feature Bypass Vulnerability. If successful, a threat actor can craft a malicious file that could go undetected by Mark of the Web (MOTW) defenses, which would result in a limited loss of integrity and availability of security features such as Protected View in Microsoft Office that rely on MOTW tagging.

- CVE-2022-41073 is a Windows Print Spooler Elevation of Privilege Vulnerability. If a threat actor can exploit this vulnerability the attacker could gain SYSTEM privileges.

- CVE-2022-41125 is a Windows Cryptographic Next Generation Key Isolation Service Elevation of Privilege Vulnerability. If a threat actor can exploit this vulnerability the attacker could gain SYSTEM privileges.

- CVE-2022-41040 is a Microsoft Exchange Server Elevation of Privilege Vulnerability that gives the attacker the ability to run PowerShell in the context of the system.

- CVE-2022-41082 is a Microsoft Exchange Server Remote Code Execution Vulnerability that gives the threat actor the ability to target the server accounts in an arbitrary or remote code execution. Once given access as an authenticated user, the threat actor could attempt to trigger malicious code in the context of the server's account through a network call.

It is important to note that Microsoft has released security updates for the two actively exploited zero-day vulnerabilities tracked as CVE-2022-41040 and CVE-2022-41082, also dubbed ProxyNotShell. Both vulnerabilities were originally disclosed in late September by cybersecurity firm GTSC.

For a complete list of Microsoft vulnerabilities released in November 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

This month Google addressed several serious issues in Android devices by issuing patches for multiple vulnerabilities that can be viewed by clicking here. Topping the list, a high-severity vulnerability in the Framework component that could lead to local escalation of privilege. Patches for November include two Google Play system updates for issues that impact the Media Framework components (CVE-2022-2209) and Wi-Fi (CVE-2022-20463). In addition to this, Google addressed five issues affecting its Pixel devices and fixed its eighth zero-day vulnerability of the year. The zero-day vulnerability, tracked as CVE-2022-4135, is a heap buffer overflow in GPU and Google is aware that an exploit for it exists in the wild. Google also issued a Stable channel update earlier this month addressing 10 Chrome vulnerabilities. Six of these flaws have a High-severity rating and include four use-after-free bugs: CVE-2022-3885, CVE-2022-3886, CVE-2022-3887, and CVE-2022-3888. The remaining two are CVE-2022-3889 which is a "type confusion" issue in V8, and CVE-2022-3890 which is a heap buffer overflow in Crashpad.

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.

Apple

Apple released security updates to address vulnerabilities in several products including Xcode. If successful, a remote threat actor could exploit these vulnerabilities and take control of a compromised device. HC3 recommends all users and administrators follow CISA's guidance which "encourages users and administrator to review Apple's security page for Xcode 14.1 and apply the necessary updates." Apple also released patches for iOS and iPadOS 16.1.1 that addresses two serious security vulnerabilities: CVE-2022-40303 and CVE-2022-40304. According to Apple's support page, both flaws are in the libxml2 software library could allow a threat actor to execute code remotely. Security updates were also released for macOS Ventura 13.0.1. 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.

Cisco

Cisco released security updates to address vulnerabilities in multiple products. If successful, a remote threat actor can exploit some of these vulnerabilities and take control of a compromised system. CISA encourages users and administrators to review the following advisories and apply the necessary updates:

- Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software SSL/TLS Client Denial of Service Vulnerability
- Cisco Secure Firewall 3100 Series Secure Boot Bypass Vulnerability
- Cisco Firepower Threat Defense Software Generic Routing Encapsulation Denial of Service Vulnerability
- Cisco FirePOWER Software for ASA FirePOWER Module, Firepower Management Center Software, and NGIPS Software SNMP Default Credential Vulnerability
- Cisco Firepower Management Center and Firepower Threat Defense Software SSH Denial of Service Vulnerability
- Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software SNMP Denial of Service Vulnerability
- Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Dynamic Access Policies Denial of Service Vulnerability

For a complete list of Cisco security advisories released, 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.

HC3: Monthly Cybersecurity Vulnerability Bulletin
December 8, 2022 TLP:CLEAR Report: 202212081200

SAP

SAP released 10 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 two vulnerabilities with severity a rating of "Hot News" which is the most severe rating. There were also two flaws classified as "High" in severity and six as "Medium." A breakdown of some security notes for vulnerabilities with "Hot News" severity rating are as follows:

- Security Note#3243924 (CVE-2022-41203) - has a 9.9 CVSS score and 'Hot News' severity rating. In some workflow of SAP BusinessObjects Business Intelligence Platform (Central Management Console and BI LaunchPad), an authenticated attacker with low privileges can intercept a serialized object in the parameters and substitute with another malicious serialized object, which leads to deserialization of untrusted data vulnerability.
- Security Note#3249990 (CVE-2021-20223 , CVE-2022-35737)- has a 9.8 CVSS score and 'Hot News' severity rating. Multiple Vulnerabilities in SQlite bundled with SAPUI5. SQLite 1.0.12 - 3.39.x before 3.39.2 can sometimes allow an array-bounds overflow if billions of bytes are used in a string argument to a C API.

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 has released security updates to address vulnerabilities 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. According to Citrix, the three vulnerabilities affecting both Citrix Gateway and Citrix ADC are the following:

- CVE-2022-27510: Critical-severity authentication bypassing using an alternate path or channel, exploitable only if the appliance is configured as VPN (Gateway).
- CVE-2022-27513: Insufficient verification of data authenticity, allowing remote desktop takeover via phishing. The flaw is exploitable only if the appliance is configured as VPN (Gateway), and the RDP proxy functionality is configured.
- CVE-2022-27516: Login brute force protection mechanism failure allowing its bypassing. This vulnerability can only be exploited if the appliance is configured as VPN (Gateway) or AAA virtual server with "Max Login Attempts" configuration.

HC3 encourages all user to follow CISA's guidance "to review Citrix Security Updates CTX463706 and apply the necessary updates" immediately.

VMWare

VMWare released eight security advisories in November. Three advisories have a 'Critical' severity rating, three 'Important,' one 'Moderate' and one has a 'Low severity rating. Additional information on some of the

severe vulnerabilities are as follows:

- VMSA-2022-0028 - This advisory has a maximum CVSSv3 base score of 9.8 and a 'Critical' severity rating. VMware Workspace ONE Assist update addresses multiple vulnerabilities: CVE-2022-31685, CVE-2022-31686, CVE-2022-31687, CVE-2022-31688, CVE-2022-31689.
- CVE-2022-31685 – VMware Workspace ONE Assist prior to 22.10 contains an Authentication Bypass vulnerability. A threat actor with network access to Workspace ONE Assist may be able to obtain administrative access without the need to authenticate to the application.
- CVE-2022-31686 - VMware Workspace ONE Assist prior to 22.10 contains a Broken Authentication Method vulnerability. A threat actor with network access to Workspace ONE Assist may be able to obtain administrative access without the need to authenticate to the application.
- CVE-2022-31687- VMware Workspace ONE Assist prior to 22.10 contains a Broken Access Control vulnerability. A threat actor with network access to Workspace ONE Assist may be able to obtain administrative access without the need to authenticate to the application.
- CVE-2022-31688 - VMware Workspace ONE Assist prior to 22.10 contains a Reflected cross-site scripting (XSS) vulnerability. Due to improper user input sanitization, a threat actor with some user interaction may be able to inject javascript code in the target user's window.
- CVE-2022-31689 - VMware Workspace ONE Assist prior to 22.10 contains a Session fixation vulnerability. A threat actor who obtains a valid session token may be able to authenticate to the application using that token.

Patches are available to remediate these vulnerabilities in affected VMware products. 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.

OpenSSL

OpenSSL released a security advisory to address two vulnerabilities (CVE-2022-3602 and CVE-2022-3786) , affecting OpenSSL versions 3.0.0 through 3.0.6. Both vulnerabilities can cause a denial of service. CVE-2022-3602 is an arbitrary 4-byte stack buffer overflow that could trigger crashes or lead to remote code execution (RCE). A threat actor could leverage CVE-2022-3786 and craft a malicious email address to overflow four attacker-controlled bytes on the stack. According to OpenSSL, "this buffer overflow could result in a crash (causing a denial of service) or potentially remote code execution," allowing a threat actor the ability to take control of a compromised system. OpenSSL also provides mitigation measures requiring administrators operating TLS servers to disable TLS client authentication until the patches are applied.

CISA encourages users and administrators "to review the OpenSSL advisory, blog, OpenSSL 3.0.7 announcement, and upgrade to OpenSSL 3.0.7." HC3 recommends all users follow CISA's guidance and apply patches immediately as all vulnerabilities can adversely impact the health sector. Additional information can be found on the 2022 OpenSSL vulnerability - CVE-2022-3602 GitHub repository that is jointly maintained by CISA and the Netherland's National Cyber Security Centrum (NCSC-NL).

Intel

Intel issued 25 security center advisories for their products in November. 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-00752 Intel NUC Firmware Advisory - Potential security vulnerabilities in some Intel NUC BIOS firmware could allow escalation of privilege or denial of service. Details on vulnerabilities with a high severity rating and their hyperlinks are as follows: CVE-2021-33164, CVE-2022-33176 CVSS 8.2 score; CVE-2022-37345 CVSS 7.8 score; CVE-2022-21794, CVE-2022-34152 CVSS 7.7; CVE-2022-32569, CVE-2022-36789, CVE-2022-35276, CVE-2022-38099, CVE-2022-26124, CVE-2022-36370 7.5 CVSS score; and CVE-2022-37334 CVSS score 7.0. Intel recommends updating the affected Intel NUC BIOS firmware to the latest version.

- INTEL-SA-00713 Intel DCM Advisory - Protection mechanism failure in the Intel DCM software before version 5.0 could allow an unauthenticated user to potentially enable escalation of privilege through adjacent access This vulnerability is tracked as CVE-2022-33942 has a CVSS base score of 8.8. Intel recommends updating the Intel DCM software to version 5.0 or later. Updates are available for download by clicking 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.

References

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

Apple Releases Security Update for Xcode
https://www.cisa.gov/uscert/ncas/current-activity/2022/11/03/apple-releases-security-update-xcode

Android Security Bulletin – November 2022
https://source.android.com/docs/security/bulletin/2022-11-01

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

Check Point Research Weekly Intelligence Report
https://research.checkpoint.com/2022/28th-november-threat-intelligence-report/

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

Citrix Releases Security Updates for ADC and Gateway
https://www.cisa.gov/uscert/ncas/current-activity/2022/11/09/citrix-releases-security-updates-adc-and-gateway

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/

CVE-2022-3786 and CVE-2022-3602: X.509 Email Address Buffer Overflows
https://www.openssl.org/blog/blog/2022/11/01/email-address-overflows/#:~:text=What%20happened%20to%20the%20CRITICAL%20vulnerability%3F

Drop What You're Doing and Update iOS, Android, and Windows
https://www.wired.com/story/ios-android-windows-vulnerability-patches-november-2022/

Google Issues Emergency Chrome Security Update for All Users
https://www.forbes.com/sites/daveywinder/2022/11/25/google-issues-emergency-chrome-security-update-for-all-users/?sh=864998241864

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

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

Microsoft November 2022 Patch Tuesday
https://isc.sans.edu/diary/rss/29230

Microsoft November 2022 Patch Tuesday fixes 6 exploited zero-days, 68 flaws
https://www.bleepingcomputer.com/news/microsoft/microsoft-november-2022-patch-tuesday-fixes-6-exploited-zero-days-68-flaws/

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

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

Open SSL Releases Security Update
https://www.cisa.gov/uscert/ncas/current-activity/2022/11/01/openssl-releases-security-update

SAP Patches Critical Vulnerabilities in Commerce, Manufacturing Execution Products
https://www.securityweek.com/sap-patches-critical-vulnerabilities-commerce-manufacturing-execution-products

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

SAP Security Patch Day – November 2022
https://securitybridge.com/sap-patchday/sap-security-patch-day-november-2022/

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

Stable Channel Update
https://chromereleases.googleblog.com/2022/11/stable-channel-update-for-desktop.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