# HC3: Monthly Cybersecurity Vulnerability Bulletin

January 10, 2022 TLP: White Report: 202201101400

## December News of Interest to the Health Sector

### Apache Log4J vulnerabilities

Several vulnerabilities were found in Apache's ubiquitous, java-based logging library, Log4J, since late November. Attacks against these vulnerabilities surged when a proof-of-concept exploit was publicly released in early December. More details can be found on these vulnerabilities below.
https://s3.documentcloud.org/documents/21120139/govuscourts22million-ransom-seizure.pdf

### FBI seized $2.3 million in cryptocurrency from REvil ransomware affiliate

In early December, it was revealed through unsealed court documentation that in August of 2021, the FBI was able to seize just under 40 bitcoins from a REvil ransomware affiliate. These bitcoins were revenues from attacks between April 2019 and June 2021, targeting both American and foreign companies.
https://s3.documentcloud.org/documents/21120139/govuscourts22million-ransom-seizure.pdf
https://www.cyberscoop.com/fbi-revil-sikerin/

### Emotet continues to recover

Emotet is a malware variant that historically has been used to attack the health sector - was disrupted and had their botnet wiped by a combined effort of the US, Canada and a number of European nations in 2021. In mid-November, a number of security companies publicly shared indications of Emotet activity again. In December, Malwarebytes as noted further spikes in Emotet activity. Specifically, they noted a 447% increase in Emotet activity beginning in November. They reported 46% of the attacks in the US, and a lot of compromised WordPress sites and as well as trojanized Windows App installers being used to deploy it.
https://blog.malwarebytes.com/trojans/2021/12/emotets-back-and-it-isnt-wasting-any-time/

### U.S. Military Has Acted Against Ransomware Groups, General Acknowledges

The US Department of Defense acknowledged for the first time the fact that they have taken offensive actions against cybercriminals. General Paul Nakasone, Chief of US Cybercommand, and the Director of the National Security Agency, acknowledged a change of philosophy in an interview with the New York Times. He noted that while previously, cybercriminals were the purview of law enforcement, after the Colonial pipeline and JBS ransomware attacks, the DoD took a more aggressive and coordinated action. The DoD has been part of actions against the REvil ransomware operators. They were also part of the effort to recover the cryptocurrency used for the ransom payment for the Colonial Pipeline attack.
https://www.nytimes.com/2021/12/05/us/politics/us-military-ransomware-cyber-command.html

### NIST releases vulnerability data for 2021

The National Institutes of Standards and Technology have released their vulnerability findings for 2021. They reported 18,378 tracked vulnerabilities for the year, the fifth straight year of record numbers.
https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time

## December Vulnerabilities of Interest to the Health Sector

### Executive Summary

In December 2021, vulnerabilities information systems relevant to the health sector have been released which 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/or patches. Vulnerabilities for this month are from Microsoft, Adobe, Android, Apache, Apple, Cisco, Google, SAP, and VMWare. HC3 recommends patching for 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

### MICROSOFT

For the month of December, Microsoft released patches for 67 new CVEs in Microsoft Windows and Windows Components, ASP.NET Core and Visual Studio, Azure Bot Framework SDK, Internet Storage Name Service, Defender for IoT, Edge (Chromium-based), Microsoft Office and Office Components, SharePoint Server, PowerShell, Remote Desktop Client, Windows Hyper-V, Windows Mobile Device Management, Windows Remote Access Connection Manager, TCP/IP, and the Windows Update Stack. This along with the 16 CVEs patched earlier this month by Microsoft Edge brings the December total to 83 CVEs; 60 of these were classified as Important and seven as Critical. In 2021, Microsoft patched 887, which is a 29% decrease from 2020. This number does not include the CVEs consumed from Chrome for the Edge (Chromium-based) browser. Some of the more important vulnerabilities for December are as follows:

- CVE-2021-43890 - **Windows AppX Installer Spoofing Vulnerability**. This patch applies to Windows' AppX installer. Microsoft reports seeing the vulnerability being used in malware in the Emotet/Trickbot/Bazaloader family. An attacker would need to craft a malicious attachment to be used in phishing campaigns and would then have to convince a user to open the malicious attachment. Code execution would occur at the local user level and the attacker would have the ability to combine this with another bug or vulnerability to take control of a target's system.
- CVE-2021-43215 – **iSNS Server Remote Code Execution Vulnerability.** This patch fixes the Internet Storage Name Service (iSNS) server vulnerability that could allow remote code execution if a hacker or threat actors sends a specially crafted request to a compromised server. Internet Storage Name Service (iSNS) is a protocol that enables automated discovery and management of iSCSI devices on a TCP/IP storage network. This means that an organization running a SAN can either leverage an iSNS server or configure each of the logical interfaces individually. This vulnerability has a CVSS rating of 9.8. HC3 recommends testing and deploying this patch immediately.
- CVE-2021-43899 – **Microsoft 4K Wireless Display Adapter Remote Code Execution Vulnerability.** This update fixes a vulnerability that could allow an unauthenticated threat or hacker to execute their code on a compromised device. The attacker would need to be on the same network as the Microsoft 4K Display Adapter at which point they could send specially crafted packets to the target's compromised device. HC3 recommends users following the vendors guidance to install the Microsoft Wireless Display Adapter application from the Microsoft Store onto a system connected to the Microsoft 4K Wireless Display Adapter. Then use the "Update & Security" section of the app to download the latest firmware to mitigate this vulnerability that also has a CVSS 9.8 rating.
- CVE-2021-43907 – Visual Studio Code WSL Extension Remote Code Execution Vulnerability. This is the third and final CVSS 9.8 vulnerability being patched for Microsoft month. While Microsoft's patch fixes a remote code execution bug in the extension, Microsoft does not specify exactly how that code execution could occur. Microsoft does however list it as unauthenticated and requires no

user interaction, so if you use this extension, HC3 recommends updating, testing, and patching immediately.

- CVE-2021-42309 – **Microsoft SharePoint Server Remote Code Execution Vulnerability.** This vulnerability allows a user to elevate and execute code in the context of the service account. A hacker or threat actor would need "Manage Lists" permissions on a SharePoint site, however by default, any authorized user can create their own new site where they have full permissions. This vulnerability allows a nefarious actor to bypass the restriction against running arbitrary server-side web control, which is similar to the previously patched CVE-2021-28474. The difference is that the unsafe control is hidden in a property of an allowed control which makes it difficult to detect.

Microsoft also fixed five publicly disclosed zero-day vulnerabilities as part of the December 2021 Patch Tuesday that are not known to be exploited in attacks.

- CVE-2021-43240 - NTFS Set Short Name Elevation of Privilege Vulnerability
- CVE-2021-41333 - Windows Print Spooler Elevation of Privilege Vulnerability
- CVE-2021-43880 - Windows Mobile Device Management Elevation of Privilege Vulnerability
- CVE-2021-43883 - Windows Installer Elevation of Privilege Vulnerability
- CVE-2021-43893 - Windows Encrypting File System (EFS) Elevation of Privilege Vulnerability

All vulnerabilities listed could adversely impact the healthcare industry and HC3 recommends patching and testing immediately. For the entire list of vulnerabilities released by Microsoft this month and their rating click here. For a list of Microsoft's December security updates click here.

## ADOBE

In December Adobe released 11 patches addressing 60 CVEs in Adobe Audition, Lightroom, Media Encoder, Premiere Pro, Prelude, Dimension, After Effects, Photoshop, Connect, Experience Manager, and Premiere Rush. The most severe of these updates impacts Adobe Experience Manager. This patch fixes eight different vulnerabilities bugs, including one rated as CVSS 9.8 and several stored cross-site scripting (XSS) issues. The Premiere Rush update fixes 16 vulnerabilities, many of them classified as Critical. The Premiere Pro patch fixes five CVEs, however one of them is a Critical-rated Out-of-Bounds (OOB) write that could allow arbitrary code execution. The specific vulnerability exists within the parsing of 3GP files, and the issue is due to a lack of proper validation of user-supplied data which can cause a read past the end of an allocated structure. The After Effects update covers 10 CVEs, including two that could allow code execution. Most of the update provides fixes for privilege escalation flaws. In addition to this, Dimension patch fixes three Critical-rated code execution vulnerabilities along with some privilege escalations. The Media Encoder patch fixes five flaws or vulnerabilities, two of them are rated Critical and if an exploit is successful could allow remote code execution. Similarly, the Prelude patch includes a fix for one Critical code execution vulnerability to go along with an Important LPE. The update for Connect addresses a single CSRF bug. Three Moderate flaws were fixed with the Adobe Audition patch and the Lightroom patch fixed one privilege escalation. The Photoshop patch fixes two Critical vulnerabilities and one with an Important rating. The Critical flaws could allow code execution if a target opens a specially crafted file.
None of the vulnerabilities fixed by Adobe in December are listed as publicly known or under active attack. 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.

# HC3: Monthly Cybersecurity Vulnerability Bulletin

January 10, 2022 TLP: White Report: 202201101400

## ANDROID

In December, Google released Android security updates for its vulnerabilities in the framework and system components along with 18 additional flaws in the kernel and vendor components in this month's security bulletin. The Android Security Bulletin provides detailed information on security vulnerabilities affecting Android devices. Security patch levels 12/5/2021 or later address all of these issues. To learn how to check a device's security patch level, see Check and update your Android version. Source code patches for these issues have been released to the Android Open-Source Project (AOSP) repository, a collection of Git repositories. CVE-2021-0967 or A-199065614 and CVE-2021-0964 or A-193363621 the high and critical severity vulnerabilities found in the Media Framework that could lead to remote information disclosure with no additional execution privileges needed. The severity assessment is based on the effect that exploiting the vulnerability would possibly have on an affected device, assuming the platform and service mitigations are turned off for development purposes or if successfully bypassed. 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. HC3 recommends users follow Android's advice which is: users should install a third-party Android distribution that will continue to deliver monthly security patches for your model or replace it with a new one. It is imperative that healthcare employees keep their devices updated, 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 such as Google Play Protect can be viewed by clicking here.

## APACHE

Several vulnerabilities have been found in Apache's ubiquitous, java-based logging library, Log4J, since late November. Attacks against these vulnerabilities surged when a proof-of-concept exploit was publicly released in early December. More details can be found on these vulnerabilities below. Log4j is a common logging framework/library, developed and maintained by the Apache Foundation and written in Java and ported to C, C++, C#, Perl, Python, Ruby, which is utilized across industries. While Java itself is becoming obsolete, there are still a lot of critical applications that rely on Log4j. There was a remote code execution vulnerability discovered in it at the end of November – CVE-2021-44228. It's been called Log4Shell or LogJam and it applies to versions 2.0-beta up to 2.14.1. The company Cloudflare reported seeing this vulnerability exploited as far back as December 1, 2021. Sophos reported seeing the vulnerability exploited by attackers dropping cryptominers. There's been some observations of the Kinsing backdoor being dropped with cryptominers as well, dropped with base64 encoded payloads and the use of shell scripts. Microsoft reported seeing Log4shell being exploited to drop Cobalt Strike, which might indicate follow-up ransomware attacks. By mid-December, additional vulnerabilities in Log4J were identified and were being aggressively exploited as well. Checkpoint reported observing almost a million attacks in a single day. CVE-2021-45046 allows an attacker to craft malicious packets in order to cause a denial of service attack. There is a vulnerability in Log4J version 1 which is a deserialization flaw and is tracked as CVE-2021-4104 and its severity is classified as high. Advanced Intelligence noted that the Conti ransomware operators – who target healthcare prolifically – are leveraging Log4J vulnerabilities in attacks. A Google report noted that they scanned the largest Java package repository (Maven Central) and found that almost 36,000 Java packages use vulnerable versions of the Log4J library. At the end of December, Sophos reported a significant drop in scanning for Log4J vulnerabilities. In late December, Apache released the most recent update to Log4J – version 2.17.1. It is a fix for a recently discovered remote code

execution vulnerability in 2.17.0 – this is tracked as CVE-2021-44832. HC3 highly recommends the following: First, HPH organizations should develop/update and review their enterprise IT asset inventory list, prioritize or triage systems and devices, and check with each associated vendor for patches. Patches should be tested and deployed aggressively. Second, situational awareness for exploitation of these vulnerabilities must also be aggressive. This includes the use of continuous monitoring tools, log analysis and endpoint security tools. No HPH organization should assume that they have not been compromised just because they are not aware of any successful attacks. Third, HPH organizations should continue to monitor Apache's official Log4J page which can be found at: https://logging.apache.org/log4j/2.x/download.html. Additional updates may be released in the coming weeks and months, and due to the high profile nature of these vulnerabilities and the ubiquitous nature Log4J, HPH organizations should continue to check this site for updated versions.

## APPLE

Apple released significant patches in December for iOS, iPadOS, macOS, tvOS and watchOS. The list of Apple security updates are as follows:

- macOS Monterey 12.1 for macOS Monterey
- macOS Big Sur 11.6.2 for macOS Big Sur
- Safari 15.2 for macOS Big Sur and macOS Catalina
- Security Update 2021-008 Catalina for macOS Catalina
- tvOS 15.2 for Apple TV 4K and Apple TV HD
- watchOS 8.3 for Apple Watch Series 3 and later
- iOS 15.2 and iPadOS 15.2 for iPhone 6s and later, iPad Pro (all models), iPad Air 2 and later, iPad 5th generation and later, iPad mini 4 and later, and iPod touch (7th generation)

For a complete list of Apple security updates click here. While none the bugs or vulnerabilities patched this month are listed as being under active attack, several of them were reported to have been used during the last Tianfu Cup. It is worth noting, that exploits at this contest has received a lot of attention in the past. HC3 recommends following Apple's recommendation of keeping software up to date and applying patches immediately. Please note, that Apple states after a software update is installed for iOS, iPadOS, tvOS, and watchOS, it cannot be downgraded to the previous version.

## CISCO

For December's patch Tuesday, Cisco released security updates for numerous products this month, including advisories related to the Log4j vulnerability in their products. Here is a list of Cisco's vulnerabilities classified as High:

- CVE-2021-33193 , CVE-2021-34798 , CVE-2021-36160 , CVE-2021-39275 , CVE-2021-40438 or Multiple Vulnerabilities in Apache HTTP Server Affecting Cisco Products: (December Update, First published November 2021) This is listed as High with a CVSS score of 9.0. An unauthenticated, remote hacker or threat actor attacker has the ability to make the httpd server forward requests to an arbitrary server due to vulnerability in the mod_proxy module of Apache HTTP Server (httpd). This flaw is caused by the incorrect handling of unix: URLs and as a result, a threat actor could exploit this vulnerability by sending a crafted HTTP request to any vulnerable device. If an exploit is successful, a hacker or threat actor can attain, modify, or delete resources on other services that may otherwise be inaccessible. For a complete list of all Cisco products that are affected by one or

more of these vulnerabilities click here.

- CVE-2021-34775 , CVE-2021-34776 , CVE-2021-34777, CVE-2021-34778, CVE-2021-34779, CVE-2021-34780 or Cisco Small Business 220 Series Smart Switches Link Layer Discovery Protocol Vulnerabilities. This is listed as High and has a CVSS rating of 8.8. Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business 220 Series Smart Switches and as result of this an unauthenticated, adjacent threat actor or hacker could execute code on the affected device or cause it to reload unexpectedly or Cause LLDP database corruption on their target's affected device. LLDP is a Layer 2 protocol and to exploit these vulnerabilities a threat actor must be in the same broadcast domain as the affected device (Layer 2 adjacent). While firmware updates have been released by Cisco to address these vulnerabilities, there are currently no workarounds to address these flaws. For more information about these vulnerabilities, you can click here.

Cisco has released a security advisory to address Cisco products affected by multiple vulnerabilities in Apache HTTP Server 2.4.48 and earlier releases. It is worth noting that an unauthenticated remote threat actor or hacker could exploit this vulnerability to take control of their target's affected system. CISA encourages users and administrators to review Cisco Advisory cisco-sa-apache-httpd-2.4.49-VWL69sWQ and apply the necessary updates. HC3 Recommends keeping software current and applying patches as soon as they are available. In addition to this, the Cisco's vulnerable products section provides Cisco bug IDs for each product. Bugs listed are accessible through the Cisco Bug Search Tool and will contain specific information, fixed software releases, and workarounds (if available).

## GOOGLE

For December's Patch Tuesday, Google provided a significant update for Chrome. The Chrome Stable channel has been updated to 96.0.4664.110, and there are five security fixes included in the patch. One of the vulnerabilities, CVE-2021-4102 which is a use-after-free bug in V8, is listed as having exploits in the wild. This month Google also addressed one Critical vulnerability along with three more High severity vulnerabilities. HC3 recommends users keep their browsers up to date. Please note that these vulnerabilities or bugs are not included in the Edge (Chromium-based) updates released on Patch Tuesday.

## SAP

For this month's Patch Tuesday, SAP released 10 Security Notes and 5 updates were previously released in Patch Day Security Notes. Click here to read SAP's statement on CVE-20211-44228 also known as "Log4Shell" a Log4j vulnerability. Four security notes were classified as Hot News and six as High Priority, details for each are as follows:

| Note# | Title | Priority | CVSS |
|---|---|---|---|
| 2622660 | *Update to Security Note released on Patch Day:*<br>**Security updates for the browser control Google Chromium delivered with SAP Business Client**<br>Product – SAP Business Client, Version – 6.5 | Hot News | 10 |
| 3109577 | **Code Execution vulnerability in SAP Commerce, localization for China**<br>Related CVEs - CVE-2021-21341,CVE-2021-21342,CVE-2021-21349,CVE-2021-21343,CVE-2021-21344,CVE-2021-21346,<br>CVE-2021-21347,CVE-2021-21350,CVE-2021-21351,CVE-2021-21345,CVE-2021-21348<br>Product - SAP Commerce, localization for China, Version - 2001 | Hot News | 9.9 |

| | | | |
|---|---|---|---|
| 3119365 | [CVE-2021-44231] **Code Injection vulnerability in SAP ABAP Server & ABAP Platform (Translation Tools)**<br>Product - SAP ABAP Server & ABAP Platform (Translation Tools), Versions - 701, 740,750,751,752,753,754, 755,756,804 | Hot News | 9.9 |
| 3089831 | *Update to Security Note released on September 2021 Patch Day:*<br>[CVE-2021-38176] **SQL Injection vulnerability in SAP NZDT Mapping Table Framework**<br>Product - SAP S/4HANA, Versions - 1511, 1610, 1709, 1809, 1909, 2020, 2021<br>Product - SAP LT Replication Server, Versions - 2.0, 3.0<br>Product - SAP LTRS for S/4HANA, Version - 1.0<br>Product - SAP Test Data Migration Server, Version - 4.0<br>Product - SAP Landscape Transformation, Version - 2.0 | Hot News | 9.9 |
| 3114134 | [CVE-2021-42064] **SQL Injection vulnerability in SAP Commerce**<br>Product - SAP Commerce, Versions - 1905, 2005, 2105, 2011 | High | 8.8 |
| 3102769 | [CVE-2021-42063] **Cross-Site Scripting (XSS) vulnerability in SAP Knowledge Warehouse**<br>Product - SAP Knowledge Warehouse, Versions - 7.30, 7.31, 7.40, 7.50 | High | 8.8 |
| 3123196 | [CVE-2021-44235] **Code Injection vulnerability in utility class for SAP NetWeaver AS ABAP**<br>Product - SAP NetWeaver AS ABAP, Versions - 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756 | High | 8.4 |
| 3077635 | [CVE-2021-40498] **Denial of service (DOS) in the SAP SuccessFactors Mobile Application for Android devices**<br>Product - SAP SuccessFactors Mobile Application (for Android devices), Versions - <2108 | High | 7.8 |
| 3124094 | [CVE-2021-44232] **Directory Traversal vulnerability in SAF-T Framework**<br>Product - SAF-T Framework, Versions - SAP_FIN 617, 618, 720, 730, SAP_APPL 600, 602, 603, 604, 605, 606, S4CORE 102, 103, 104, 105 | High | 7.7 |
| 3113593 | **Denial of service (DOS) in SAP Commerce**<br>Related CVE - CVE-2021-37714<br>Product - SAP Commerce, Versions - 1905, 2005, 2105, 2011 | High | 7.5 |

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.* For a full list of SAP security notes click here.

## VMWARE

**In December's Patch Tuesday VMWare** released an advisory regarding current patches for the Log4j vulnerability in their products. CVE-2021-44228 and CVE-2021-45046 were identified as Critical vulnerabilities in Apache Log4j that impact VMware products. There are numerous VMWare e products impacted by remote code execution vulnerabilities through the Apache Log4j vulnerabilities CVE-2021-44228 and CVE-2021-45046. Threat actors or hackers with network access to a compromised VMware product could possibly exploit these issues to gain full control of their target's system. You can access "fixes" and "workarounds" for CVE-2021-44228 and CVE-2021-45046 by clicking here and scrolling down to the 'Fixed Version' column of the 'Response Matrix'. This is an ongoing event; HC3 recommends that VMWare users to check for frequent updates, keep software update, and to apply patches immediately.

## Recently Published Information

Adobe Joins Security Patch Tuesday Frenzy
https://www.securityweek.com/adobe-joins-security-patch-tuesday-frenzy

Android and Google service mitigations

https://source.android.com/security/bulletin/2021-12-01#mitigations

Android Security Bulletin—December 2021
https://source.android.com/security/bulletin/2021-12-01

Microsoft Patch Tuesday, December 2021 Edition –
https://krebsonsecurity.com/2021/12/microsoft-patch-tuesday-december-2021-edition/

Microsoft December 2021 Patch Tuesday fixes 6 zero-days, 67 flaws
https://www.bleepingcomputer.com/news/microsoft/microsoft-december-2021-patch-tuesday-fixes-6-zero-days-67-flaws/

The December 2021 Security Update Review –
https://www.zerodayinitiative.com/blog/2021/12/14/the-december-2021-security-update-review

Windows 10 KB5008212 & KB5008206 updates released
https://www.bleepingcomputer.com/news/microsoft/windows-10-kb5008212-and-kb5008206-updates-released/

## 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