HC3: Monthly Cybersecurity Vulnerability Bulletin

February 4, 2022 TLP: White Report: 202202041200

January News Items of Interest to the Health Sector

FBI: Hackers target US defense firms with malicious USB packages

The FBI released a flash alert warning US companies that the cybercriminal group FIN7 targeted the US defense industry with infected USB devices to deploy ransomware. FIN7 impersonated Amazon and the US Department of Health and Human Services and mailed packages containing USB drives with the LilyGO logo containing malware such as 'BadUSB' or 'Bad Beetle USB' . They targeted the transportation and insurance industries since August 2021 and defense firms starting in November 2021. Since August, these packages also contain letters about COVID-19 guidelines or counterfeit gift cards and forged thank you notes.

Number of Major Health Data Breaches in 2021

Health Care Info Security analyzed the data breach numbers reported to HHS for 2021 and they noted the following:

- In 2021, there were a total of 713 health data breaches affecting more than 45.7 million individuals
- Breaches caused by Hacking/IT incidents were the most prevalent
- This total represents a noticeable increase from 2020 when there were 663 breaches affecting more than 34 million individuals in 2020 (very rough numbers, 10% increase in breaches and 30% increase in number of people impacted)
- These numbers represent the most individuals in a single year impacted since 2015. However, in 2015, there was a single incident with the health insurance company Anthem, which involved exposure of almost 80M individual records, bringing the total for that year over 112M.

Interpol arrests 11 BEC gang members linked to 50,000 targets

Interpol announced that they, in coordination with the Nigerian Police Force, arrested 11 individuals suspected of participating in an international BEC (business email compromise) ring. The name of their gang is SilverTerrier; They are alleged to have collectively been involved in BEC criminal schemes possibly associated with more than 50,000 targets. One of the arrested suspects was in possession of more than 800,000 potential victim domain credentials on his laptop.

Russian government arrests REvil ransomware gang members

The Russian Federal Security Service) arrested 12 members of the REvil (AKA Sodinokibi) ransomware gang. They detained a total of 14 suspected REvil members or affiliates and confiscated both cryptocurrency and fiat money which included more than 426 million rubles (approximately $5.5 million), 600,000 US dollars and 500,000 euros (approximately $570,000). They also confiscated 20 luxury cars purchased with money obtained from cyberattacks, computer equipment and cryptocurrency wallets.

HC3: Monthly Cybersecurity Vulnerability Bulletin

February 4, 2022 TLP: White Report: 202202041200

January Vulnerabilities of Interest to the Health Sector

Executive Summary

In January 2022, vulnerabilities in common 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 come from Microsoft, Adobe, Android, Google, Apple, Cisco, Citrix, Intel, Mozilla, 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, device hygiene, and asset tracking are imperative to an effective patch management program.

Importance to HPH Sector

DEPARTMENT OF HOMELAND SECURITY/CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

In January, 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 January, Microsoft patched 126 vulnerabilities including six zero-days. Microsoft has fixed problems including remote code execution (RCE) exploits, privilege escalation flaws, spoofing issues, and cross-site scripting (XSS) vulnerabilities. There were 24 vulnerabilities patched earlier this month in Microsoft Edge (Chromium-based). Products that are affected by this month's security update include Microsoft Exchange Server, the Office software line, Windows Defender, Windows Kernel, RDP, Cryptographic Services, Windows Certificate, and Microsoft Teams. The six zero-day vulnerabilities released in Microsoft's updates for this month are as follows:

- CVE-2021-22947: This is an open source Curl RCE allowing for Man-in-The-Middle (MiTM) attacks.
- CVE-2021-36976: An open source Libarchive use-after-free bug leading to RCE.
- CVE-2022-21874: A local Windows Security Center API RCE vulnerability.
- CVE-2022-21919: A Windows User Profile Service Elevation of Privilege security issue.
- CVE-2022-21839: Windows Event Tracing Discretionary Access Control List Denial-of-Service (DoS) (CVSS 6.1).
- CVE-2022-21836: Windows Certificate spoofing.

At the time the patches were released, none of the zero-day vulnerabilities listed above were known to have been actively exploited in the wild. Additional noteworthy vulnerabilities for this month are:

- CVE-2022-21907 is a HTTP Protocol Stack Remote Code Execution Vulnerability with a severity rating of 9.8 Critical.
- CVE-2022-21846 is Microsoft Exchange Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-21855, CVE-2022-21969. It has a severity rating of 9.0 Critical.

Microsoft published an emergency fix earlier this month for a vulnerability impacting on-premises Exchange Servers that was a date-check failure glitch that kept mail from moving smoothly through the transport queues of Exchange Server 2016 and Exchange Server 2019. Microsoft has announced e security update guide notification system that accepts standard email addresses during signup rather than only Live IDs. HC3 recommends patching and testing immediately as all vulnerabilities can adversely impact the healthcare industry. For the entire list of vulnerabilities released by Microsoft this month and their rating click here.

ADOBE

In January Adobe released security updates for multiple products. Some products of note are as follows:

- APSB22-01 – This updates Acrobat and Reader for Windows and macOS to address multiple critical, important, and moderate vulnerabilities. Successful exploitation could lead to arbitrary code execution, memory leak, application denial of service, security feature bypass and privilege escalation.
- APSB22-03 – This applies to Adobe Bridge and addresses critical, important, and moderate vulnerabilities that could lead to arbitrary code execution and privilege escalation.
- APSB22-04 – This applies to Adobe InCopy and addresses important and critical vulnerabilities.
- APSB22-05 – This applies to Adobe InDesign and addresses moderate as well as critical vulnerabilities.

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 take control of a compromised system.

ANDROID / GOOGLE

The Android Security Bulletin provides detailed information on security vulnerabilities affecting Android devices. For the month of January, it describes 35 vulnerabilities addressed across two patch levels, the majority of these listed with a High severity level. The first portion of the Android security update, the 2022-01-01 security patch level, addressed 16 security holes for three components: Framework, Media Framework, and System. The second portion of the Android security update, the 2022-01-05 security patch level, provides fixes for 19 security defects in the following: Android runtime, Kernel components, MediaTek components, Unisoc components, Qualcomm components, and Qualcomm closed-source components. The most severe high security vulnerability is CVE-2021-0959, an Android runtime flaw that impacts devices running Android 12, because it could allow a local attacker or threat actor to bypass memory restrictions in order to gain access to additional permissions. 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.

HC3: Monthly Cybersecurity Vulnerability Bulletin

February 4, 2022 TLP: White Report: 202202041200

APPLE

For the month of January, Apple has released security updates to address CVE-2022-22588, a vulnerability affecting iOS 15.2.1 and iPadOS 15.2.1. If successful with processing a maliciously crafted HomeKit accessory name, a threat actor may be able to cause a denial of service. HC3 recommends following Apple's recommendation of keeping software up to date and applying patches immediately. Administrators and users are urged to visit the Apple security updates page for more information on iOS 15.2.1 and iPadOS 15.2.1 and apply the necessary updates. For a complete list of Apple security updates click here. According to Apple, after a software update is installed for iOS, iPadOS, tvOS, and watchOS, it cannot be downgraded to the previous version.

CISCO

Cisco patched five vulnerabilities (CVE-2021-33193, CVE-2021-34798 , CVE-2021-36160, CVE-2021-39275, and CVE-2021-40438). These vulnerabilities affect the Apache HTTP Server (httpd) 2.4.48 and earlier releases and were originally disclosed in September 2021. CISCO is encouraging users to upgrade to an appropriate fixed software release by clicking here. When considering software upgrades, users are advised to regularly consult the advisories for Cisco products located on the Cisco Security Advisories page to determine exposure and a complete upgrade solution. 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. All vulnerabilities are accessible through the Cisco Bug Search Tool and will contain specific information, fixed software releases, and workarounds (if available).

CITRIX

Citrix released several security updates to address vulnerabilities in Hypervisor (CVE-2021-28704, CVE-2021-28705, CVE-2021-28714, and CVE-2021-28715.) Administrators are also advised to review Citrix Security Update CTX335432. The latest version of Citrix Workspace app for Linux is available and can be found here.

DRUPAL

Drupal released security updates to address vulnerabilities affecting Drupal 7, 9.2, and 9.3. An attacker could exploit these vulnerabilities to take control of an affected system. They can be found in their security advisories, SA-CORE-2022-001. and SA-CORE-2022-002.

INTEL

Intel released a security advisory for Apache Log4j2 vulnerabilities CVE-2021-44228 and CVE-2021-45046. The severity rating for CVE-2021-44228 is 10.0 and it is classified as Critical. JNDI features in Apache Log4j2 may allow an authenticated user to potentially enable escalation of privilege via network access. CVE-2021-45046 is classified as Critical with a base score of 9.0. It was found that the fix to address CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete in certain non-default configurations. HC3 recommends following Intel's guidance, which is to update Intel products listed here to the latest mitigated version indicated on the table. In addition to this, Intel recommends using the Apache Log4j mitigations or workarounds for any affected products that cannot be updated or that do not have an updated product version that can be found here.

HC3: Monthly Cybersecurity Vulnerability Bulletin

February 4, 2022 TLP: White Report: 202202041200

IVANTI

Ivanti updated its Log4j Advisory with security updates for multiple products to address CVE-2021-44228. An unauthenticated attacker could exploit this vulnerability to take control of an affected system. Also, CISA encourages users and administrators to review the Ivanti security advisories pages for Avalanche; File Director; and MobileIron Core, MobileIron Sentry (Core/Cloud), and MobileIron Core Connector and apply the necessary updates and workarounds.

F5

F5 released a list of patched vulnerabilities that can be found here. The two most important of those are CVE-2022-23008 which affects their NGINX Controller API Management (versions 3.18.0 - 3.19.0) and CVE-2022-23009 which affects BIG-IQ Centralized Management (8.0.0 version) products.

MOZILLA

Mozilla released security updates for vulnerabilities in Firefox, Firefox ESR, and Thunderbird. This included security advisories for Firefox 96, Firefox ESR 91.5, and Thunderbird 91.5.

ORACLE

Oracle released their 2022 Q1 vulnerability bulletin in January and it can be found here. This bulletin contains 497 new security patches across many of their product families. Information on Log4J vulnerabilities in Oracle products can be found here.

SAMBA

The Samba Team has released a security update to address a vulnerability in multiple versions of Samba. An attacker could exploit this vulnerability to take control of an affected system. Details can be found in their announcement for CVE-2021-43566.

SAP

SAP published a security note 3131047 that consolidated all security notes addressing recent vulnerabilities related to Apache Log4j 2 component. SAP also released 11 new security notes, 16 out-of-band notes, and 3 updates to previously released notes. Users can find additional SAP guidance at their Support Portal. The entire list of security notes released by SAP in January can be found here.

VMWARE

VMWare released five security advisories this month. One is classified Critical, two as Important, and two as Moderate. These include Apache Log4j Remote Code Execution Vulnerabilities CVE-2021-44228 and CVE-2021-45046, a VMware Tools workaround addressing a local privilege escalation vulnerability CVE-2020-3941, and a VMware Workstation, Fusion, and ESXi update addressing a heap-overflow vulnerability CVE-2021-22045. A complete list of VMWare Security advisories can be found here.

ZOHO

Zoho has released a security advisory to address an authentication bypass vulnerability (CVE-2021-44757) in ManageEngine Desktop Central and Desktop Central MSP. An attacker could exploit this vulnerability to take control of an affected system.

HC3: Monthly Cybersecurity Vulnerability Bulletin

February 4, 2022 TLP: White Report: 202202041200

Recently Published Information

Adobe Releases Security Updates for Multiple Products
https://www.cisa.gov/uscert/ncas/current-activity/2022/01/11/adobe-releases-security-updates-multiple-products

Apple Releases Security Updates for iOS and iPadOS
https://www.cisa.gov/uscert/ncas/current-activity/2022/01/13/apple-releases-security-updates-ios-and-ipados

CISA alerts federal agencies of ancient bugs still being exploited
https://www.bleepingcomputer.com/news/security/cisa-alerts-federal-agencies-of-ancient-bugs-still-being-exploited/

Citrix Releases Security Updates for Hypervisor
https://www.cisa.gov/uscert/ncas/current-activity/2022/01/13/citrix-releases-security-updates-hypervisor

Citrix Workspace App for Linux Security Update
https://support.citrix.com/article/CTX338435

Drupal Releases Security Updates
https://www.cisa.gov/uscert/ncas/current-activity/2022/01/20/drupal-releases-security-updates

Ivanti Updates Log4j Advisory with Security Updates for Multiple Products
https://www.cisa.gov/uscert/ncas/current-activity/2022/01/14/ivanti-updates-log4j-advisory-security-updates-multiple-products

January 2022 Security Updates
https://msrc.microsoft.com/update-guide/releaseNote/2022-Jan

Juniper Networks Releases Security Updates for Multiple Products
https://www.cisa.gov/uscert/ncas/current-activity/2022/01/13/juniper-networks-releases-security-updates-multiple-products

K40084114: Overview of F5 vulnerabilities (January 2022)
https://support.f5.com/csp/article/K40084114

Microsoft Patch Tuesday – January 2022
https://isc.sans.edu/forums/diary/Microsoft+Patch+Tuesday+January+2022/28230/

Mozilla Releases Security Updates for Firefox, Firefox ESR, and Thunderbird
https://www.cisa.gov/uscert/ncas/current-activity/2022/01/11/mozilla-releases-security-updates-firefox-firefox-esr-and

Oracle Critical Patch Update Advisory - January 2022
https://www.oracle.com/security-alerts/cpujan2022.html

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

Security update available for Adobe Acrobat and Reader | APSB22-01
https://helpx.adobe.com/security/products/acrobat/apsb22-01.html

WordPress Releases Security Update
https://www.cisa.gov/uscert/ncas/current-activity/2022/01/07/wordpress-releases-security-update

Wormable' Flaw Leads January 2022 Patch Tuesday
https://krebsonsecurity.com/2022/01/wormable-flaw-leads-january-2022-patch-tuesday/

Zoho Releases Security Advisory for ManageEngine Desktop Central and Desktop Central MSP
https://www.cisa.gov/uscert/ncas/current-activity/2022/01/19/zoho-releases-security-advisory-manageengine-desktop-central-and

Intelligence Insights: January 2022 Log4j target found in VMware Horizon, new BLISTER loader may contain Cobalt Strike beacons, and ManageEngine exploitation continues
https://redcanary.com/blog/intelligence-insights-january-2022/

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