HC3: Monthly Cybersecurity Vulnerability Bulletin

November 17, 2021 TLP: White Report: 202111171300

News of Interest to the Health Sector

FinCEN report: Top 10 ransomware groups responsible for 5.2 billion in transactions

The U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) released a report on ransomware. They examined 177 cryptocurrency addresses tied to the top 10 ransomware groups and concluded that they have extorted a total of $5.2 billion dollars. In the first half of 2021 – these 10 groups extorted a total of $1.56 billion. FinCEN is currently tracking 68 active ransomware groups. They assessed that Bitcoin is the most common cryptocurrency used for ransomware payments.
https://www.fincen.gov/sites/default/files/shared/Financial%20Trend%20Analysis_Ransomeware%20508%20FINAL.pdf

President Biden announced 30-country coalition against ransomware

The Biden administration convened a meeting of 30 countries to attempt to collaborate and crackdown on ransomware operators. Specifically, these efforts are going to include improving law enforcement collaboration and reducing the illicit use of cryptocurrency as well as engaging on a diplomatic level
https://www.cnn.com/2021/10/01/politics/blinken-cybersecurity-alliance/index.html

Man sentenced to 7 years in prison for hacking healthcare provider

Justin Sean Johnson, known online as TheDearthStar and Dearthy Star, was sentenced last month to seven years in prison for the 2014 hack of the University of Pittsburgh Medical Center He was convicted of having breached UPMC's human resources databases, stealing personally identifiable information (PII) and W-2 info (including names, Social Security numbers, addresses and salary information) associated with over 65,000 employees and sold it on the dark web. Last year, he was charged in a forty-three-count indictment for conspiracy, wire fraud, and aggravated identity theft. Earlier this year, he pleaded guilty to stealing and selling the PII and W2 info of tens of thousands of UPMC employees.
https://www.bleepingcomputer.com/news/security/man-gets-7-years-in-prison-for-hacking-65k-health-care-employees/

ThycoticCentrify: 2021 State of Ransomware Survey & Report

The cybersecurity company ThycoticCentrify released their "2021 State of Ransomware Survey & Report" and for it, they surveyed 300 US-based IT decision-makers. They found that 64% of those organizations have been victims of a ransomware attack in the last 12 months, and 83% of those attack victims paid the ransom demand. Half of the respondents said they experienced a loss of revenue and reputational damage from a ransomware attack, while 42% indicated they had lost customers as a result of an attack. More than 30% said they were forced to lay off employees. Finally, respondents said the most vulnerable vectors for ransomware attacks were email (53%), followed by applications (41%) and the cloud (38%).
https://www.zdnet.com/article/83-of-ransomware-victims-paid-ransom-survey/

Cyberattack on Alabama hospital linked to 1st alleged ransomware death

According to a lawsuit filed against Springhill Medical Center of Mobile Alabama, a ransomware attack that caused the facility to shut down its network for almost eight days is alleged to have caused the death of a newborn baby. The lawsuit alleges the ransomware attack disrupted the monitoring of the baby's heart rate, as that baby had medical complications, this ultimately caused the baby to lose its life.
https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116

HC3: Monthly Cybersecurity Vulnerability Bulletin

November 17, 2021 TLP: White Report: 202111171300

Vulnerabilities of Interest to the Health Sector

Executive Summary

In October 2021, 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 are Microsoft, Adobe, Android, Apache, Apple, Cisco, Google, SAP, and VMWare. HC3 recommended 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.

MICROSOFT

For the month of October, Microsoft fixed 74 vulnerabilities, 81 total including Microsoft Edge, and four zero-day vulnerabilities. Three of these flaws are categorized as Critical, 70 are Important, and one as Low. These 81 vulnerabilities (including Microsoft Edge) are classified as: 21 Elevation of Privilege; 6 Security Feature Bypass; 20 Remote Code Execution; 13 Information Disclosure; 5 Denial of Service; and 9 Spoofing. This month, Microsoft fixed the final PrintNightmare but it was followed by a wide-scale of printing problems. Details for 4 of critical vulnerabilities from Microsoft's Patch Tuesday:

CVE-2021-40449 - Win32k Elevation of Privilege Vulnerability - known to have been actively exploited in the wild. According to Kaspersky, this vulnerability has been used before by threat actors who, during the attack, would install a remote access trojan (RAT) that was elevated with higher permissions using this vulnerability. This cluster of malicious activity is called MysterSnail and it is attributed to the IronHusky and Chinese-speaking APT activity. Microsoft rates this as Exploitation Detected on the latest software release on the Exploitability Index.

CVE-2021-40469 - Windows DNS Server Remote Code Execution Vulnerability - This vulnerability is a remote code execution within the Microsoft DNS server that affects all operating systems from Server 2008 to Server 2022. Servers with the DNS Server role configured are only impacted by this flaw. This is rated as Exploitation Less Likely by Microsoft.

CVE-2021-41335 - Windows Kernel Elevation of Privilege Vulnerability – This CVE, a publicly disclosed vulnerability in the Windows Kernel could lead to privilege escalation. It does not include Windows 11 and Windows Server 2022 as CVE-2021-40449 flaw. This is also rated Exploitation Less Likely by Microsoft.

CVE-2021-41338 - Windows AppContainer Firewall Rules Security Feature Bypass Vulnerability. This vulnerability was discovered by Google Project Zero's James Forshaw who posted his research here. This is rated as Exploitation Less Likely by Microsoft. Microsoft issued an update in their October Security Guidance: ADV200011 – Microsoft Guidance for Addressing Security Feature Bypass in GRUB, which indicates that newer versions of Windows, including Windows 11, are affected and that an update will be released to address this in Spring 2022. For the entire list of vulnerabilities released by Microsoft in October click here. All of these vulnerabilities can potentially adversely impact the healthcare industry and HC3 recommends patching and testing immediately. For Microsoft guidance and future updates click here

HC3: Monthly Cybersecurity Vulnerability Bulletin

November 17, 2021 TLP: White Report: 202111171300

ADOBE

Adobe issued security updates for 92 vulnerabilities in 14 products, with 66 of them classified as Critical security vulnerabilities. Patched products include Reader and Acrobat, Commerce, After Effects, Audition, Bridge, Premiere Pro, Premiere Elements, the XMP Toolkit SDK, Framemaker document processor and Connect. Some of these are as follows:

Premiere Elements:

- CVE-2021-40785 (*NULL Pointer Dereference/memory leak*)
- CVE-2021-40786, CVE-2021-40787, CVE-2021-42526, CVE-2021-42527 (Access of Memory Location After End of Buffer/ACE)

Premiere Pro:

- CVE-2021-40792, CVE-2021-40793, CVE-2021-40794 (Access of Memory Location After End of Buffer/ACE)

XMP Toolkit SDK:

- CVE-2021-42529, CVE-2021-42530, CVE-2021-42531, CVE-2021-42532 (Stack-Based Buffer Overflow/ACE)

While Adobe has fixed the privilege escalation, arbitrary code execution (ACE), denial-of-service and memory leaks/information disclosure issues; users should also take additional steps to ensure their devices are secure. HC3 recommends that users apply the appropriate security updates or patches that can be found on Adobe's Product Security Incident Response Team (PSIRT) by clicking here. The SANS Internet Storm Center has a review of the patches released and their severity levels here.

ANDROID

In October, Google released Android security updates for 41 vulnerabilities, ranging between high and critical severity. None of the vulnerabilities addressed have been reported as being exploited in the wild. These vulnerabilities affect Qualcomm closed-source components. HC3 recommends healthcare organizations, especially those who maintain a bring your own device (BYOD) policy review these. The three critical severity flaws in the set are tracked as:

- CVE-2021-0870: Which is a remote code execution flaw in Android System, enabling a remote attacker to execute arbitrary code within the context of a privileged process.
- CVE-2020-11264: This is critical flaw that impacts Qualcomm's WLAN component, concerning the acceptance of non-EAPOL/WAPI frames from unauthorized peers received in the IPA exception path.
- CVE-2020-11301: This is a critical flaw that affects Qualcomm's WLAN component, concerning the acceptance of unencrypted (plaintext) frames on secure networks.

For a complete list of Android's vulnerabilities click here and Qualcomm's vulnerabilities click here.

Older Android devices that are no longer supported with security updates now have an increased attack surface, because some vulnerabilities fixed are ideal for threat actors to create working exploits in the future. It is also worth noting, that Android security patches are not just for Android versions, and the fixes are for Android versions 8.1 to Android 11. The operating system (OS) version is not a determining factor in whether or not a device is still supported. If a device has reached the end of life (EOL) date, 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 views by clicking here.

APACHE

For October, Apache reported 2 critical vulnerabilities. The first vulnerability, CVE-2021-41773, was introduced by a change made to path normalization in Apache HTTP Server 2.4.49, therefore its earlier versions are not vulnerable. Servers that are configured to "require all denied" are not vulnerable either but is set to off in the default configuration. This is the setting that typically shows an error that looks like this: *"Forbidden. You don't have permission to access {path}."* The second vulnerability CVE-2021-41524— a null pointer dereferences detected during HTTP/2 request processing. This flaw allows an attacker to perform a denial of service (DoS) attack on the server. This requires a specially crafted request. This CVE only exists in Apache Server version 2.4.49, however it is different to the first vulnerability because it not under active exploitation. It was discovered and fixed late and incorporated version 2.4.50. For mitigation, HC3 recommends all system administrators follow the Apache guidance: those that have not installed 2.4.49 yet should skip this version in their update cycle and go straight to 2.4.50, and users that have 2.4.49 installed should configure "require all denied" if they do not plan to patch quickly, since this blocks the attack that has been seen in the wild. The comprehensive list of vulnerabilities in Apache HTTP Server 2.4 can be found here.

APPLE

Apple released security updates for iOS and iPadOS in October that included an actively exploited zero-day vulnerability. iOS 15.0.2 and iPadOS 15.0.2 was released by Apple to fix the zero-day vulnerability (CVE-2021-30883) that is being leveraged in active attacks targeting iPhone and iPad users. This can impact the Healthcare industry if employees are using these devices for work or to access sensitive data and their device is compromised. This an integer overflow vulnerability in the iOS "IOMobileFrameBuffer" component can allow an application to execute arbitrary code with kernel privileges and is accessible from the browser. This vulnerability can be used by a hacker or threat actor steal data or install malware. Older Apple models and devices without current Apple iOS make up the majority of devices compromised.

Apple released security updates for the following: iOS 15.0.1 and iPadOS 15.0.1 , iOS 15.0.2 and iPadOS 15.0.2, watchOS 8.0.1 (CVE details not published yet), tvOS 15.1 , iOS 15.1 and iPadOS 15.1, watchOS 8.1 , Security Update 2021-007 Catalina , macOS Monterey 12.0(Preinstalled only on certain Mac models; update to macOS Monterey 12.0.1), macOS Big Sur 11.6.1, macOS Monterey 12.0.1 *(Advisory includes security content of macOS Monterey 12.0 and macOS Monterey 12.0.1),* iOS 14.8.1 and iPadOS 14.8.1, and Safari 15.1 To mitigate this threat, HC3 recommends that all users install the latest version of version of Apple iOS and apply the latest security patches. For a complete list of Apple security updates click here.

CISCO

Cisco Talos identified a use-after-free vulnerability in the ConditionalFormatting functionality of Microsoft Office Excel 2019 that could allow an attacker to execute arbitrary code on the victim machine. The vulnerability CVE-2021-40474 also known as TALOS-2021-1259 can be exploited by a hacker or threat

actor if they are successful in convincing their target to open an Excel file. Proper heap grooming by the threat actor could provide them with full access and control of this use-after-free vulnerability and it could also lead to an arbitrary code execution.

HC3 recommends following the vendors recommendation, which is users are advised to update the following software affected by this vulnerability: Microsoft Office Excel 2019 x86, version 2101, build 13628.20448 and Office Excel 365 x86, version 2008, build 13127.21216. SNORT rules 52417 and 52418 will detect exploitation attempts against this vulnerability. Additional rules may be released in the future and current rules are subject to change, pending additional vulnerability information. Cisco Talos and Microsoft worked together to resolve this issue and have provided an update for affected customers, which can be accessed by clicking here.

GOOGLE

For the third consecutive month, Google has fixed two previously unknown 'zero-day' bugs in their desktop browser. Google stated they patched the two high-severity zero-day flaws in release notes for the stable release of Chrome version 95.0.4638.69 for Windows, Mac and Linux; version numbers higher than that will already have the fixes. CVE-2021-38000 and CVE-2021-38000 are the two zero-day flaws that are actively being exploited by attackers now. They were discovered by Google's Threat Analysis Group (TAG), which tracks state-sponsored and cyber-criminal exploit activity. On October 26th the second of the two zero-days were also reported by Samuel Groß from Google Project Zero.

- CVE-2021-38000 was originally reported by TAG on September 15th. It is a design flaw caused by "insufficient validation of untrusted input in Intents."
- CVE-2021-38003 is a memory corruption flaw described as "inappropriate implementation in V8."

In addition to this, there were eight (mostly memory-related) security fixes in October's Chrome update. On the list of high-severity flaws: a use-after-free in Sign-in, another use-after-free in Chrome's garbage collection, insufficient data validation in Chrome's New Tab page, a type confusion in V8, and a use-after-free in Web Transport. Google Project Researcher Groß plans on using V8 Heap Sandbox also referred to as "Ubercage" to stop these attacks and provide protections. According to the proposal, "To protect other memory in the same process from corruption, and by extension prevent the execution of arbitrary code, all raw pointers in the V8 heap are converted into either offset into a virtual memory "cage" or indices into an external pointer table."

Google's October 28th release notes said, "Google is aware that exploits for CVE-2021-38000 and CVE-2021-38003 exist in the wild," and that their update roll out will be over the coming days or weeks. Google has patched a high number of zero-day flaws in Chrome in 2021. In addition to this, there has been a significant increase in zero-days affecting Chrome, Windows, and iOS over the past year. These platforms are used in the Healthcare industry, so it is imperative for users to be aware of any risks or vulnerabilities. HC3 recommends patching immediately and visit Google's support page for Chrome updates and details on how Chrome can be set to automatically update when patches become available.

SAP

In October SAP released 17 new and updated SAP Security Notes on its October 2021 patch release, with 4 of them listed as critical. As part of this month's patch release, there are three HotNews notes and one High Priority note. HC3 recommends patching immediately and following SAP's guidance. For a full list of

SAP security notes click here.

VMWARE

VMWare provided two security updates for the month of October. The first is to address VMware vRealize Operations to addresses SSRF Vulnerability (CVE-2021-22033) vRealize Operations contains a Server Side Request Forgery (SSRF) vulnerability and the severity of this issue has been evaluated by VMware and is considered to be in the Low severity range with a maximum CVSSv3 base score of 2.7. With this type of vulnerability, a malicious actor that has gained administrative access to vRealize Operations can enumerate internal IPs and internal ports. VMware vRealize Operations, VMware Cloud Foundation, and vRealize Suite Lifecycle Manager are all products impacted by this vulnerability. To remediate this issue, HC3 recommends applying patches listed in the 'Fixed Version' section of the 'Response Matrix' which can be accessed by clicking here.

The second security update is to address VMware vRealize Log Insight updates address Comma Separated Value(CSV) injection vulnerability (CVE-2021-22035). VMware vRealize Log Insight has a CSV injection vulnerability in interactive analytics export function. This impacts the following products: VMware vRealize Log Insight; VMware Cloud Foundation, and vRealize Suite Lifecycle Manager. VMware has listed this CVE as being in the Moderate severity range with a maximum CVSSv3 base score of 6.5. With this vulnerability an authenticated threat actor with non-administrative privileges could be able to embed untrusted data prior to exporting a CSV sheet through Log Insight which could be executed in user's environment. To remediate this issue, HC3 recommends applying the patches listed in the 'Fixed Version' column of the 'Response Matrix' which can be accessed by clicking here. A SSRF vulnerability in VMware vRealize Operations was privately reported to VMware. Patches are available to address this vulnerability in affected VMware products.

References

Microsoft October 2021 Patch Tuesday fixes 4 zero-days, 71 flaws
https://www.bleepingcomputer.com/news/microsoft/microsoft-october-2021-patch-tuesday-fixes-4-zero-days-71-flaws/

Microsoft Patch Tuesday for Oct. 2021 — Snort rules and prominent vulnerabilities
https://blog.talosintelligence.com/2021/10/microsoft-patch-tuesday-for-oct-2021.html

https://www.zdnet.com/article/microsoft-october-2021-patch-tuesday-71-vulnerabilities-four-zero-days-squashed/
Microsoft October 2021 Patch Tuesday: 71 vulnerabilities, four zero-days squashed

Microsoft October 2021 Patch Tuesday
https://isc.sans.edu/forums/diary/Microsoft+October+2021+Patch+Tuesday/27928/

THE OCTOBER 2021 SECURITY UPDATE REVIEW
https://www.zerodayinitiative.com/blog/2021/10/12/the-october-2021-security-update-review

ICS Patch Tuesday: Siemens and Schneider Electric Address Over 50 Vulnerabilities

https://www.securityweek.com/ics-patch-tuesday-siemens-and-schneider-electric-address-over-50-vulnerabilities

Patch Tuesday, October 2021 Edition
https://krebsonsecurity.com/2021/10/patch-tuesday-october-2021-edition/

October Patch Tuesday: 3 Critical Bulletins Among 71
https://www.trendmicro.com/en_us/research/21/j/october-patch-tuesday-3-critical-bulletins-among-71.html

VERT Threat Alert: October 2021 Patch Tuesday Analysis
https://www.tripwire.com/state-of-security/featured/vert-threat-alert-october-2021-patch-tuesday-analysis/

October Security Update: It's Cybersecurity Awareness Month
https://www.devprojournal.com/technology-trends/security/october-security-update-its-cybersecurity-awareness-month/

Apple fixes iOS zero-day exploited in the wild (CVE-2021-30883)
https://www.helpnetsecurity.com/2021/10/12/cve-2021-30883/

Vulnerability Spotlight: Use-after-free vulnerability in Microsoft Excel could lead to code execution
https://blog.talosintelligence.com/2021/10/vuln-spotlight-excel-code-execution.html

Apple silently fixes iOS zero-day, asks bug reporter to keep quiet
https://www.bleepingcomputer.com/news/apple/apple-silently-fixes-ios-zero-day-asks-bug-reporter-to-keep-quiet/

SAP Patches Critical Vulnerabilities in Environmental Compliance
https://www.securityweek.com/sap-patches-critical-vulnerabilities-environmental-compliance

SAP Security Patch Day – October 2021
https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=587169983

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

VMware Security Solutions: Advisories - VMSA-2021-0021
https://www.vmware.com/security/advisories/VMSA-2021-0021.html

VMware Security Solutions: Advisories - VMSA-2021-0022
https://www.vmware.com/security/advisories/VMSA-2021-0022.html