HC3: Monthly Cybersecurity Vulnerability Bulletin

December 15, 2021 TLP: White Report: 202112151200

November News of Interest to the Health Sector

US and International Law Enforcement Crackdown on Cybercriminals

November saw increased action by both US and international law enforcement and partner organizations against cybercriminal groups, many of whom target healthcare. Early in the month, Europol detained several suspects. Their accusations include launching cyberattacks against 1800 victim organizations in 71 countries since 2019. The arrests involved efforts by eight countries, including the United States.
https://www.europol.europa.eu/newsroom/news/12-targeted-for-involvement-in-ransomware-attacks-against-critical-infrastructure
https://therecord.media/europol-detains-suspects-behind-lockergoga-megacortex-and-dharma-ransomware-attacks/

The US Department of State announced a $10 million reward for the identification of key DarkSide ransomware members and $5 million for information leading to the arrest of participants. This group is believed to be behind the Colonial pipeline ransomware attack in May of 2021.
https://www.bleepingcomputer.com/news/security/us-targets-darkside-ransomware-rebrands-with-10-million-reward/

Romanian law enforcement arrested two suspects believed to be REvil ransomware affiliates. Kuwaiti authorities arrested a GandCrab (predecessor to REvil) ransomware affiliate, the three of them are suspected of launching roughly 7,000 attacks and demanding over $200 million total in ransoms.
https://www.europol.europa.eu/newsroom/news/five-affiliates-to-sodinokibi/revil-unplugged

The US Department of Justice indicted two individuals associated with the REvil ransomware group. One of those individuals was arrested in Poland, which maintains an extradition treaty with the United States. They also announced they seized more than $6M in cryptocurrency from one of the indicted operators.
https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya

The US Department of State announced a reward of up to $10 million for information leading to the identification or location of any individual holding a key leadership position in the REvil ransomware group.
https://www.state.gov/reward-offers-for-information-to-bring-sodinokibi-revil-ransomware-variant-co-conspirators-to-justice/

The US Treasury Department announced sanctions on the cryptocurrency exchange Chatex for “facilitating financial transactions for ransomware actors.”
https://home.treasury.gov/news/press-releases/jy0471

Russian national Aleksandr Zhukov, aka the "King of Fraud”, was arrested in Bulgaria in 2018 and extradited to the United States in 2019. He was charged, convicted and in early November 2021 sentenced to 10 years in prison and ordered to forfeit $4 million in assets for operating the large-scale digital advertising fraud scheme 'Methbot' that stole at least $7 million from American companies.
https://www.justice.gov/usao-edny/pr/russian-cybercriminal-sentenced-10-years-prison-digital-advertising-fraud-scheme

HC3: Monthly Cybersecurity Vulnerability Bulletin

December 15, 2021 TLP: White Report: 202112151200

Interpol announced a coordinated law enforcement operation against cybercrime that resulted in the arrest of over 1,000 individuals, the freezing of 2,350 bank accounts linked to online crimes, and the interception of nearly $27M of illicit funds. This was called Operation HAECHI-II and it took place from June to September 2021, with the joint efforts of specialized police units from 20 countries, predominantly in South America, Europe and Southeast Asia.
https://www.interpol.int/News-and-Events/News/2021/More-than-1-000-arrests-and-USD-27-million-intercepted-in-massive-financial-crime-crackdown

The FBI recently revealed through unsealed court documentation that in August 2021, they were able to seize just under 40 bitcoins from a REvil ransomware affiliate's Exodus wallet, which is the equivalent of about $2.3M at current prices
https://s3.documentcloud.org/documents/21120139/govuscourts22million-ransom-seizure.pdf

Emotet is back:

Emotet, a malware variant that has been around since 2014 and used prolifically to target healthcare targets in cyberspace (among other industries), was disrupted earlier this year by law enforcement but the cybercriminal group behind it appears to be attempting to reconstitute the infrastructure behind it. Security researchers and companies have been releasing small indications of its activity on social media. They are reporting that Emotet has made updates to its capabilities such as changes to the loader and new commands are available for it as well as for the dropper. In addition to this, here is a new command and control infrastructure operational and there are reportedly already 246 systems that are part of it.
https://www.bleepingcomputer.com/news/security/emotet-malware-is-back-and-rebuilding-its-botnet-via-trickbot/

H-ISAC paper:

The Health Information Sharing and Analysis Center (H-ISAC) published the paper: ***Identity, Interoperability, Patient Access and the 21st Century Cures Act: A Health-ISAC Guide for CISOs***
This paper is intended to help healthcare CISOs implement an identity-centric approach to cybersecurity by understanding how an identity-centric approach to securing and enabling access to electronic health information will allow health organizations to minimize risks involved in complying with the 21st Century Cures Act.
https://h-isac.org/interoperability-for-healthcare-cisos/

MITRE released a Playbook for Threat Modeling Medical Devices

MITRE released a playbook for threat modeling medical devices which is intended to serve as a resource for developing or evolving medical device threat modeling. It is methodologies-agnostic and focuses on the basic principles of threat modeling.
https://www.mitre.org/publications/technical-papers/playbook-threat-modeling-medical-devices

HC3: Monthly Cybersecurity Vulnerability Bulletin

December 15, 2021 TLP: White Report: 202112151200

November Vulnerabilities of Interest to the Health Sector

Executive Summary

In November 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, Cisco, and SAP. 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.

MICROSOFT

For the month of November Microsoft fixed six zero-day vulnerabilities and a total of 55 flaws. A zero-day is computer software vulnerability that is publicly disclosed or actively exploited with no official patch or fix available. Of the 55 vulnerabilities Microsoft fixed, 49 were classified as Important and six as Critical. A breakdown of the vulnerabilities are as follows:

- 20 Elevation of Privilege vulnerabilities
- 2 Security Feature Bypass vulnerabilities
- 15 Remote Code Execution vulnerabilities
- 10 Information Disclosure vulnerabilities
- 3 Denial of Service vulnerabilities
- 4 Spoofing vulnerabilities

Both Microsoft Exchange and Excel have actively exploited vulnerabilities, with the Exchange zero-day used in the Tianfu hacking contest. The actively exploited vulnerabilities fixed this month are as follows:

- CVE-2021-42292 – *Microsoft Excel Security Feature Bypass Vulnerability* – This is the Microsoft Excel vulnerability that was identified by the Microsoft Threat Intelligence Center as actively being used in malicious attacks The patch for this CVE fixes a bug that has the ability to allow code execution when opening a specially crafted file with an affected version of Excel. This is more than likely due to loading code that should be behind a prompt that does not appear which allows it to bypass that security feature. Researchers are trying to determine whether or not this is a malicious macro or another version of code loading within a spreadsheet. To be safe it is best to open attachment only from sources you trust. There is currently no patch available for Office of Mac users. It is working noting that although Microsoft lists this CVE as currently under active attack, the CVSS rating lists the exploit code maturity as "proof of concept."
- CVE-2021-42321 - *Microsoft Exchange Server Remote Code Execution Vulnerability*- This is the Exchange vulnerability that is an authenticated remote code execution bug. In *October it was used as part of the Tianfu Cup hacking contest.* Microsoft listed this vulnerability currently under active

attack and the authentication is listed as a requirement. It recommended that Exchange administrators or users test and deploy the patches as soon as possible.

Two additional CVE's with noteworthy updates are as follows:

- CVE-2021-26443 – Microsoft Virtual Machine Bus (VMBus) Remote Code Execution Vulnerability – The patch for this CVE addresses a guest-to-host escape through the virtual machine bus (VMBus). A guest VM user has the ability to send a specially crafted communication on the VMBus channel to the host OS that could create an arbitrary code execution on the underlying host. This CVE is one of the more severe vulnerabilities fixed this month and has a CVSS rating of 9.0.
- CVE-2021-38666 – Remote Desktop Client Remote Code Execution Vulnerability – this vulnerability is in the RDP client and while not as severe as the CVE in the RDP server, is still considered a CVE to monitor. If a user is lured by a threat actor to connect to a malicious RCP server, they could execute code on the connecting RDP client system.

These four other publicly disclosed vulnerabilities, that are not known to be exploited in attacks, were also fixed by Microsoft:

- CVE-2021-38631 - Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability
- CVE-2021-41371 - Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability
- CVE-2021-43208 - 3D Viewer Remote Code Execution Vulnerability
- CVE-2021-43209 - 3D Viewer Remote Code Execution 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 in November click here. For Microsoft guidance and future updates click here.

ADOBE

In November Adobe released three patches, corrected four critical vulnerabilities and exposures (CVEs) in Creative Cloud Desktop, InCopy, and RoboHelp. The details for these patches are as follows:
Creative Cloud - The patch for Creative Cloud fixes a single Important-rated denial-of-service (DoS) bug.
InCopy - The InCopy patch fixes two bugs, including a Critical-rated code execution.
RoboHelp Server - RoboHelp Server's release is listed as a security hotfix instead of a security patch. While they are similar, the takeaway here is that a Critical-rated arbitrary code execution bug is fixed and if you used RoboHelp you should apply this hotfix. No patches released by Adobe in November are listed as being 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.

ANDROID

In November, Google released Android security updates for 18 vulnerabilities in the framework and system components along with 18 additional flaws in the kernel and vendor components. The list of fixes for the month are as follows:

- CVE-2021-1048 - This is local escalation of privilege that is caused by a "use after free weakness" (CWE-416). According to Google this is under limited, targeted exploitation. Original equipment manufacturers (OEMs) are working on merging the patch with their custom builds, which means most Android users are vulnerable.

- CVE-2021-0918 and CVE-2021-0930 – These two critical System remote code execution (RCE) bugs are the most severe issues addressed by Android this month. These vulnerabilities allow threat actors the ability to execute arbitrary code within the context of a privileged process sending a specially crafted transmission to the target's device.

- CVE-2021-1924 and CVE-2021-1975 are both critical security flaws impacting Qualcomm components.

- CVE-2021-0889 is the fifth critical flaw that impacts Android TV's "remote service" component. A malicious actor near the device could exploit this vulnerability and would have the ability to execute code without privileges or user interaction.

While this is the first security patch for Android 12, many of the fixes go back to versions 11, 10, and 9. Anyone using older Android versions are not covered by this patch level and your device is vulnerable. This is the first patch level not delivered to Pixel 3, which marks the official end of support for the Google device. 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.

cisco

In November Cisco released a patch to fix multiple vulnerabilities in cisco products. Here is a list of Cisco's vulnerabilities classified as Critical and High:

- CVE-2021-40119: This critical CVE is a SSH keys vulnerability in Cisco Policy Suite Static can allow an unauthenticated, remote attacker to log in to an affected system as the root user. This vulnerability caused by to the re-use of static SSH keys across installations.
- CVE-2021-34795: This critical CVE is a vulnerability located in the web-based management interface of the Cisco Catalyst PON Series Switches can allow an attacker to perform command injection, configuration changes and Log in with a default credential if the Telnet protocol is enabled on affected systems. This vulnerability is caused by the insufficient expiration of session credentials.
- CVE-2021-34739: This CVE is classified as High and is session credentials replay vulnerability located in Cisco Small Business Series Switches and it can give a threat actor or hacker the ability to replay valid user session credentials and gain unauthorized access to web-based management interface with administrator privileges.

- CVE-2021-34741: This CVE is classified as High and is Denial of Service (DoS) vulnerability in Cisco Email Security Appliance that allows a threat actor or hacker the ability to perform a denial of service (DoS) attack against an affected device. This vulnerability is caused by insufficient input validation of incoming emails.

A remote threat actor or hacker's successful exploit of critical vulnerabilities can give them control of the affected system as the root user. HC3 recommends users update Cisco products with latest available patches.

SAP

For this month's Patch Tuesday, SAP released 5 Security Notes and provided 2 updates to previously released Patch Day Security Notes. Here is a list of the top 3 priority security notes released this month:

- *Hot New Priority* Note 3099776 or CVE-2021-40501 is a SAP ABAP Platform Kernel vulnerability in versions 7.77, 7.81, 7.85, 7.86. These versions do not perform necessary authorization checks for an authenticated business user and can result in an escalation of privileges. This essentially means the business user is able to read and modify data beyond the vulnerable system. In addition to this, a threat actor can neither significantly reduce the performance of the system nor stop the system. It has a CVSS rating of 9.6.
- *High Priority* Note 3110328 or CVE-2021-40502 is a SAP Commerce vulnerability in versions 2105.3, 2011.13, 2005.18, 1905.34. These versions do not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. Threat actors or hackers can be erroneously authenticated and will be able to access and edit data from b2b units they do not belong to. It has a CVSS rating of 8.3.
- *High Priority* Note 2971638 or CVE-2020-6369 is a SAP Solution Manager and SAP Focused Run CVE (update provided in WILY_INTRO_ENTERPRISE 9.7, 10.1, 10.5, 10.7). This vulnerability allows a threat actor or an unauthenticated attacker the ability to bypass the authentication process if the default passwords for Admin and Guest have not been changed by the administrator and that could affect the confidentiality of the service. It is also worth noting that this is an update to Security Note released on October 2020 Patch it has a CVSS rating of 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.

INTEL

Intel disclosed two high-severity vulnerabilities that affect several of their processor families. Both of these allow for a potential escalation of privilege attack. These processors are included in systems widely deployed across many industries, including the healthcare and public health sector. Vulnerabilities They vulnerabilities are tracked as CVE-2021-0157 and CVE-2021-0158, with each having a CVSS score of 8.2 out of 10.

References

Android November patch fixes actively exploited kernel bug
https://www.bleepingcomputer.com/news/security/android-november-patch-fixes-actively-exploited-kernel-bug/

HC3: Monthly Cybersecurity Vulnerability Bulletin

December 15, 2021 TLP: White Report: 202112151200

Android Security Bulletin
https://source.android.com/security/bulletin/2021-11-01

ICS Patch Tuesday: Siemens and Schneider Electric Address Over 50 Security Flaws
https://www.securityweek.com/ics-patch-tuesday-siemens-and-schneider-electric-address-over-50-vulnerabilities-0

Microsoft CVE Summary
https://rawcdn.githack.com/campuscodi/Microsoft-Patch-Tuesday-Security-Reports/f18c781b4406271bd289b4f2f112f9e4c7b27de5/Reports/MSRC_CVEs2021-Nov.html

Microsoft November 2021 Patch Tuesday fixes 6 zero-days, 55 flaws
https://www.bleepingcomputer.com/news/microsoft/microsoft-november-2021-patch-tuesday-fixes-6-zero-days-55-flaws/

THE NOVEMBER 2021 SECURITY UPDATE REVIEW
https://www.zerodayinitiative.com/blog/2021/11/9/the-november-2021-security-update-review

SAP Security Patch Day – November 2021
https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=589496864

Windows 11 KB5007215 update released with application fixes
https://www.bleepingcomputer.com/news/microsoft/windows-11-kb5007215-update-released-with-application-fixes/

Microsoft urges Exchange admins to patch bug exploited in the wild
https://www.bleepingcomputer.com/news/microsoft/microsoft-urges-exchange-admins-to-patch-bug-exploited-in-the-wild/

Released: November 2021 Exchange Server Security Updates
https://techcommunity.microsoft.com/t5/exchange-team-blog/released-november-2021-exchange-server-security-updates/ba-p/2933169?WT.mc_id=M365-MVP-5003086

November 2021 Patch Tuesday forecast: More mandates in the United States
https://www.helpnetsecurity.com/2021/11/08/november-2021-patch-tuesday-forecast/

Microsoft November 2021 Patch Tuesday: 55 bugs squashed, two under active exploit
https://www.zdnet.com/article/microsoft-november-2021-patch-tuesday-55-bugs-patched-two-under-active-exploit/

Microsoft November 2021 Patch Tuesday
https://isc.sans.edu/forums/diary/Microsoft+November+2021+Patch+Tuesday/28018/

Microsoft Patch Tuesday, November 2021 Edition
https://krebsonsecurity.com/2021/11/microsoft-patch-tuesday-november-2021-edition/

Microsoft Nov. Patch Tuesday Fixes Six Zero-Days, 55 Bugs
https://threatpost.com/microsoft-nov-patch-tuesday-fixes-six-zero-days-55-bugs/176143/

Microsoft Fixes Exchange Server Zero-Day

https://www.darkreading.com/vulnerabilities-threats/microsoft-s-nov-security-update-contains-fix-for-exchange-server-0-day

November 2021 Patch Tuesday falls back to just 57 bug fixes
https://news.sophos.com/en-us/2021/11/09/november-2021-patch-tuesday-falls-back-to-just-57-bug-fixes/

Microsoft: November 2021 Security Updates
https://msrc.microsoft.com/update-guide/releaseNote/2021-Nov

Microsoft patches actively exploited Exchange, Excel zero-days (CVE-2021-42321, CVE-2021-42292)
https://www.helpnetsecurity.com/2021/11/09/cve-2021-42321-cve-2021-42292/

Exchange Server bug: Patch now, but multi-factor authentication might not stop these attacks, warns Microsoft
https://www.zdnet.com/article/exchange-server-bug-patch-now-but-mfa-might-not-stop-these-attacks-warns-microsoft/

Microsoft patches Excel zero-day used in attacks, asks Mac users to wait
https://www.bleepingcomputer.com/news/microsoft/microsoft-patches-excel-zero-day-used-in-attacks-asks-mac-users-to-wait/

Patch Tuesday updates the Win 7 updater… for at most 1 more year of updates
https://nakedsecurity.sophos.com/2021/11/10/patch-tuesday-updates-the-win-7-updater-for-at-most-1-more-year-of-updates/

Microsoft Patch Tuesday for Nov. 2021 — Snort rules and prominent vulnerabilities
https://blog.talosintelligence.com/2021/11/microsoft-patch-tuesday-for-nov-2021.html

Intel BIOS Reference Code Advisory
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00562.html

Intel chip flaw could enable attacks on laptops, cars, medical devices (CVE-2021-0146)
https://www.helpnetsecurity.com/2021/11/15/intel-chip-flaw-cve-2021-0146/

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