LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF INFORMATION SECURITY

HC3: Monthly Cybersecurity Vulnerability Bulletin

October 15, 2021 TLP: White Report: 202110151400

News of Interest to the Health Sector

BrakTooth - The BrakTooth vulnerabilities were first made public on August 31, 2021, after being discovered by the ASSET Research Group. This new family of security vulnerabilities, found in commercial Bluetooth Classic stacks for various System-on-Chips (SoC),uses the Bluetooth Classic (BR/EDR) protocol and affects millions of Bluetooth-enabled devices. BrakTooth vulnerabilities pose a threat to the Healthcare and Public Health (HPH) sector because the risk associated with the BrakTooth set of security flaws ranges from denial-of-service (DoS) by crashing the device firmware, or a deadlock condition where Bluetooth communication is no longer possible, to arbitrary code. It is recommended that Healthcare Delivery Organizations (HDOs), Healthcare Professionals and manufacturers reach out to the ISAC/ISAOs for assistance with responding.

Conti Ransomware - Conti is a ransomware group that has aggressively targeted the healthcare industry, major corporations, and government agencies, particularly those in North America since it was first observed in 2019. During this type of cyber-attack, the threat actor steals sensitive data from compromised networks, encrypts the targeted organizations' servers and workstations, and threatens to publish the stolen data unless the target pays a ransom. According to the Joint Cybersecurity Advisory from CISA and the FBI, they have observed the increased use of Conti ransomware in more than 400 attacks on U.S. and international organizations, at least 16 of which have targeted US healthcare and related organizations. To secure systems against Conti ransomware, CISA/NSA/FBI recommends implementing the recommended mitigations in the advisory.

Hardening Remote Access VPN - The NSA and CISA issued a joint information sheet providing guidance on hardening Virtual Private Networks (VPNs) services because remote access VPN servers are entry points into protected networks and have become targeted by malicious actors. The healthcare industry uses VPN technologies for telehealth, telemedicine, patient access to records and appointments as well as a variety of other applications. The NSA and CISA advises selecting standards-based VPNs from reputable vendors with a proven track record of quickly remediating vulnerabilities and following best practices in regard to using strong authentication credentials.
Compromise can lead to the disruption of healthcare operations and leaking of sensitive health information, including research-related intellectual property as well as protected employee and patient information, leading to a leak of personal health information (PHI) and a potential HIPAA violation. HC3 recommends that healthcare organizations review the NSA/CISA joint information sheet and take appropriate actions in accordance with their risk management strategy.

Medusa TangleBot – Medusa (AKA TangleBot) is a malware spreading via SMS and is targeting Android mobile users by sending COVID-19 related SMS messages with a malicious link to trick victims into installing Medusa/TangleBot onto their devices then collecting data and installing additional malware. Once the malware infects a device, it can use a multitude of data gathering capabilities, including accessing the victim's internet, call logs, GPS, and using the victim's device to spread malware throughout the mobile network. This is concerning if someone in the Healthcare industry's mobile work device is compromised because once the malware is installed onto a device it can be difficult to detect and remove. Currently, warning messages from Android appear to be the best option available to protect mobile devices from infection. HC3 recommends ensuring enterprise Android device users are made aware of this threat and that everyone only clicks links or download applications(apps) that are reputable.

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF INFORMATION SECURITY

HC3: Monthly Cybersecurity Vulnerability Bulletin

October 15, 2021 TLP: White Report: 202110151400

New Azure AD Brute Force - A newly discovered bug in Microsoft Azure's Active Directory implementation enables a single-factor brute-forcing of an Active Directory instance without authentication. Currently there is no available patch for this vulnerability. This vulnerability is expected to impact the health sector due to the fact that Microsoft Active Directory technology is ubiquitous and, as such, is heavily utilized. The nature of this vulnerability allows for compromise with minimal possibility of detection and the lack of a patch makes it further challenging, leaving administrators and network defenders with minimal visibility into an attacker's actions. HC3 recommends healthcare organizations take mitigation actions in accordance with their unique risk posture and continue to monitor for patches or further recommendations.

Vulnerabilities of Interest to the Health Sector for the month of September

Executive Summary

In September 2021, vulnerabilities in common information systems relevant to the healthcare sector have been released which require prioritized 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 as they are developed. Vulnerabilities for this month are from Microsoft, WordPress, Sonic Wall, VMWare, OMI, Mozilla, Conti, Citrix, CISCO, Chrome, Matrix, Arcadyan, Apple, and Adobe. All vulnerabilities should be considered for patching with special consideration to each vulnerability criticality category against the risk management posture of the organization. Accountability, proper inventory management and asset tracking are vital to an effective patch management program.

MICROSOFT

Microsoft released patches for 66 CVEs in Microsoft Windows and Windows components, Microsoft Edge (Chromium, iOS, and Android), Azure, Office and Office Components, SharePoint Server, Microsoft Windows DNS, and the Windows Subsystem for Linux. There were 20 CVEs patched by Microsoft Edge (Chromium-based) earlier in the month, bringing the September total to 86 vulnerabilities. Below are some noteworthy updates from Microsoft for September:

- CVE-2021-40444 - **Microsoft MSHTML Remote Code Execution Vulnerability**
  This patch fixes a bug currently being exploited through Office documents. A specially crafted ActiveX control is embedded in an Office doc then sent to a target. If opened on an affected system, code executes at the level of the logged-on user. Microsoft lists disabling ActiveX as a workaround, but other reports state this may be ineffective. The CVSS for this vulnerability is 8.80 (out of 10). At this time, the most effective defense is to apply the patch and avoid Office documents that you do not anticipate receiving. There are multiple updates for specific platforms, be sure to carefully review and install all needed patches to ensure you are covered.
- CVE-2021-38647 - **Open Management Infrastructure Remote Code Execution Vulnerability**
  This patch rates the highest CVSS (9.8) for September and fixes an RCE bug in the Open Management Infrastructure (OMI). OMI is an open-source project to further the development of a production-quality implementation of the DMTF CIM/WBEM standards. This vulnerability does not require user interaction or privileges, so an attacker can run their code on an affected system by sending a specially crafted message to an affected system. This is a critical vulnerability in Microsoft Open Management Infrastructure (CVE-2021-38647) and users should test and deploy

patches immediately. This open-source project led by Microsoft implements web-based enterprise management standards and the vulnerability may be used for remote code execution. The CVSS for this vulnerability is 9.80 and you can read more about OMI by clicking here.

- CVE-2021-36965 - **Windows WLAN AutoConfig Service Remote Code Execution Vulnerability**
A remote code execution affecting Windows WLAN AutoConfig Service was fixed (CVE-2021-36965). This vulnerability affects almost all supported Windows versions, may be exploited by an attacker on an adjacent network, requires no privilege and no user interaction. This patch fixes a vulnerability that could allow network adjacent attackers to run their code on affected systems at SYSTEM level. This means an attacker could completely take over the target – provided they are on an adjacent network. HC3 recommends applying patches and testing immediately. (For visuals of this data click here)

ADOBE

Adobe released 15 patches for 59 CVEs in Adobe Acrobat Reader, XMP Toolkit SDK, Photoshop, Experience Manager, Genuine Service, Digital Editions, Premiere Elements, Photoshop Elements, Creative Cloud Desktop, ColdFusion, Framemaker, InDesign, SVG-Native-Viewer, InCopy, and Premiere Pro. The Zero Day Initiative (ZDI) program discovered 17 of those vulnerabilities.

Adobe Acrobat provided fixes for a total of 26 bugs this month - the most severe could allow remote code execution through either a heap-based buffer overflow, type confusion, or a use after free vulnerability. The single bug fixed by the Photoshop patch could also lead to code execution when opening a specially crafted file. The most severe of these issues are due to the lack of proper validation of user-supplied data, which could result in a memory corruption condition. It is recommended users patch the two Critical rated security feature bypass bugs immediately. A list of Adobe's patches is available on their PSIRT page.
(For visuals or graphics of Adobe Security updates click here)

APPLE

Apple's patches included an urgent security update to fix a "zero-click" iOS vulnerability (CVE-2021-30860) reported by researchers that allows arbitrary commands to be run. CVE-2021-30860 fixes an input validation bug in CoreGraphics that could allow remote code execution. Experts found an exploit for CVE-2021-30860 was being used by the NSO Group, an Israeli tech company whose spyware enables the remote surveillance of smartphones. In addition to this, CVE-2021-30858 – a Use-After-Free (UAF) bug in Webkit – has also been detected in the wild. These bugs impact several different Apple products, including iOS, iPad OS, watchOS, Safari, Catalina, and Big Sur. CISA encourages users and administrators to review the Apple security pages for the following products and apply the necessary updates: Safari 15, Xcode 13, watchOS 8, iOS 15, iPadOS 15 , and iTunes 12.12 for Windows. HC3 recommends patching , testing, and applying the necessary updates immediately.

ARCADYAN

A path traversal vulnerability, identified as CVE-2021-20090, was discovered in numerous routers manufactured by multiple vendors using Arcadyan based software. What makes this vulnerability unique is that it allows an unauthenticated user access to sensitive information and allows for the alteration of the router configuration. Arcadyan-based routers and modems are vulnerable to authentication bypass and an unauthenticated attacker is able to use this vulnerability to access protected resources.

Successful exploitation of this vulnerability gives an unauthenticated threat actor or attacker access to pages and data that requires authentication. The unauthenticated attacker compromising a system could gain access to sensitive data, including valid request tokens, which can be used to alter router settings. The CERT/CC recommends updating your router to the most recent firmware available and disabling the remote (WAN-side) administration services on any SoHo router and web interface on the WAN.

MATRIX

The Matrix Foundation released an advisory September 13, 2021, stating a vulnerability was discovered by one of its researchers during a routine audit. The critical security issue, tracked as CVE-2021-40823 and CVE-2021-40824, is due to a logic error in the room key sharing functionality of Matrix and is an implementation bug in certain Matrix clients and SDKs which support end-to-end encryption ("E2EE"). Exploiting this vulnerability to read encrypted messages requires gaining control over the recipient's account by either compromising their credentials directly or their home server. A critical vulnerability of this nature in certain Matrix clients could allow an attacker access to encrypted messages. This vulnerability affects multiple Matrix clients and libraries including Element (Web/Desktop/Android), FluffyChat, Nheko, Cinny, and SchildiChat. Element on iOS is not affected. Patched versions of affected clients are available now. It is recommended that users update to the latest versions immediately.

GOOGLE

Google released a new version of its Chrome browser this month fixing nine vulnerabilities, including two listed as under active attack. CVE-2021-30632 fixes an Out-of-Bounds (OOB) Write, while CVE-2021-30633 fixes a UAF bug. The CVE's could lead to code execution at the level of the logged-on user. All of the bugs fixed in this release received a "High" severity rating from Google. If you are running Chrome, update to ensure you are on the latest stable version and also be mindful of the "Update" button that is on the right of the address bar as it will signal whether or not your browser is up to date. You may see the "Update" button turn from green to orange and then red if you have had your browser open for an extended period of time. The color *green* signifies that an update has been available for two days; *orange* means four days have elapsed, and seeing *red* means that your browser is a week or more behind on important updates. HC3 recommends closing and restarting the browser to install any pending updates.

CISCO

Cisco has released security updates to address September vulnerabilities in multiple Cisco products. Cisco's updates includes a full list of fixes for 31 bugs; more than one dozen of them rated with a high-severity score or worse. A threat actor or attacker could exploit some of these vulnerabilities to take control of an affected system. At the top of the list in terms of severity is CVE-2021-34770, which is a vulnerability that could be exploited remotely by an unauthenticated attacker to run arbitrary code with root privileges. Cisco has patched three critical vulnerabilities affecting components in its IOS XE internetworking operating system powering routers and wireless controllers, or products running with a specific configuration. The worst of the flaws received 10 out of 10; the highest severity rating. It affects the Cisco Catalyst 9000 Family Wireless Controllers that includes the enterprise-class Catalyst 9800-CL Wireless Controllers for Cloud. Another critical-severity vulnerability with a score (9.8/10) caused by insufficient bounds checking is in the vDaemon process in Cisco IOS XE SD-WAN Software, now identified as CVE-2021-34727. During this attack, a threat actor or hacker can leverage remotely without authentication by sending modified traffic to a vulnerable target device. Successful exploitation could lead to executing arbitrary commands with the highest privileges or at least cause a denial-of-service (DoS) condition. These products are vulnerable if they are running on an outdated version of Cisco IOS XE SD-WAN software with the SD-WAN feature active (disabled by default):

- 1000 Series Integrated Services Routers (ISRs)
- 4000 Series ISRs
- ASR 1000 Series Aggregation Services Routers
- Cloud Services Router 1000V Series

Cisco also patched critical bug CVE-2021-1619. It is a security issue in the authentication, authorization, and accounting (AAA) function of Cisco IOS XE software. A remote threat actor could use it to install, manipulate, or delete the configuration of an affected device. A successful exploit could allow the attacker to use NETCONF or RESTCONF to install, manipulate, or delete the configuration of a network device or to corrupt memory on the device, possibly causing a DoS. CISA encourages users to review the following Cisco advisories and apply the necessary updates: Cisco IOS XR Software for ASR 9000 Series Routers Denial of Service Vulnerability | Cisco IOS XR Software IP Service Level Agreements and Two-Way Active Measurement Protocol Denial of Service Vulnerability | Cisco IOS XR Software Arbitrary File Read and Write Vulnerability | Cisco IOS XR Software Authenticated User Privilege Escalation Vulnerabilities
You can see updates addressing lower severity vulnerabilities, on the Cisco Security Advisories page.

CITRIX

Citrix has released security updates to address vulnerabilities in Hypervisor. An attacker could exploit these vulnerabilities to take control of an affected system. CISA encourages users and administrators to review Citrix Security Update CTX325319 and apply the necessary updates. Several security issues have been discovered in Citrix Hypervisor that, collectively, may allow privileged code in a guest VM to compromise or crash the host. These issues have the following identifiers which can be viewed by clicking on their CVE-ID: CVE-2021-28694 , CVE-2021-28698 (Host Denial of Service) CVE-2021-28697 , CVE-2021-28699 , CVE-2021-28701 (Host Compromise) All currently supported versions of Citrix Hypervisor are affected by all of these issues with the exception of CVE-2021-28699 which only affects Citrix Hypervisor 8.2 LTSR. Citrix has released hotfixes and recommends customers install them and patch immediately. The hotfixes can be downloaded clicking on Citrix Hypervisor 8.2 LTSR: CTX324257 or Citrix Hypervisor 7.1 LTSR CU2: CTX324256.

MOZILLA

Mozilla has released security updates to address vulnerabilities in Firefox, Firefox ESR, and Thunderbird. An attacker could exploit some of these vulnerabilities to take control of an affected system. CISA encourages users and administrators to review the Mozilla security advisories for Firefox 92, Firefox ESR 78.14, and Thunderbird 78.14.

OMI

This month Microsoft's Security Response Center (MSRC) released security patches for four critical vulnerabilities affecting the Microsoft Azure package Open Management Infrastructure (OMI). The open-source OMI package was created to provide a portable infrastructure backbone such as diagnostic monitoring, log analytic services and automation functionality within UNIX and Linux systems for web-based management tools. OMI is used by Microsoft Azure to manage UNIX packages within Azure virtual machines (VMs), containers and serverless cloud instances. The four critical vulnerabilities discovered by security researchers from Wiz include one unauthenticated remote code execution (RCE) and three privilege escalation vulnerabilities. (CVE-2021-38645 – Privilege Escalation vulnerability | CVE-2021-38647 – Unauthenticated RCE as root | CVE-2021-38648 – Privilege Escalation vulnerability | CVE-2021-38649 – Privilege Escalation vulnerability)

These four vulnerabilities also referred to as OMIGOD, were found to directly affect Azure cloud instances using the following Azure services: Azure Automation, Azure Automatic Update, Azure Operations Management Suite, Azure Log Analytics, Azure Configuration Management, and Azure Diagnostics. Prisma Cloud Compute Defender can detect whether an Azure system is vulnerable to any of the four CVEs. It is recommended that Prisma Cloud users build a custom vulnerability detection rule to identify if any system is running an OMI package a version prior to 1.6.8.1. In addition to this, any system created or has updated its OMI package after August 11, 2021 should be patched immediately.

VMWARE

On September 21, 2021 VMware disclosed its vCenter Server was affected by CVE-2021-22005, an arbitrary file upload vulnerability in the Analytics service. This means that a malicious threat actor with network access to port 443 can exploit the vulnerability to execute code on vCenter Server. On September 24, 2021 VMware confirmed reports of CVE-2021-22005 being exploited in the wild. In addition to this, researchers are reporting mass scanning for vulnerable vCenter Servers and publicly available exploit code. CISA expects widespread exploitation of this vulnerability due to the availability of exploit code. To mitigate CVE-2021-22005, CISA strongly urges critical infrastructure entities and other organizations with affected vCenter Server versions: 1) Upgrade to a fixed version as quickly as possible. See VMware Security Advisory VMSA-2021-0020 for patching information and 2) Apply the temporary workaround provided by VMware, if unable to upgrade to a fixed version immediately. See VMware's workaround instructions for additional CVE-2021-22005, for additional information.

SONIC WALL

SonicWall has patched a critical security flaw impacting several Secure Mobile Access (SMA) 100 series products that can let unauthenticated attackers remotely gain admin access on targeted devices. The SMA 100 series appliances vulnerable to attacks targeting the improper access control vulnerability tracked as CVE-2021-20034 includes SMA 200, 210, 400, 410, and 500v. Successful exploitation can let attackers delete arbitrary files from unpatched SMA 100 secure access gateways to reboot to factory default settings and potentially gain administrator access to the device.

SonicWall SMA 100 series appliances have been targeted by ransomware gangs' multiple times since the start of 2021, with the end goal of moving laterally into the target organization's network. SonicWall recently revealed that its products are used by more than 500,000 business customers in over 215 countries and territories worldwide. Many of them are deployed on the networks of the world's largest organizations, enterprises, and government agencies.For instance, a threat group Mandiant tracks as UNC2447 exploited the CVE-2021-20016 zero-day bug in SonicWall SMA 100 appliances to deploy a new ransomware strain known as FiveHands (a DeathRansom variant just as HelloKitty).

There are no temporary mitigations to remove the attack vector, and SonicWall strongly urges impacted customers to deploy security updates that address the flaw as soon as possible.

WORDPRESS

WordPress 5.4-5.8 are affected by multiple vulnerabilities. An attacker could exploit these vulnerabilities to take control of an affected website. CISA encourages users and administrators to review the WordPress Security and Maintenance Release and upgrade to WordPress 5.8.1. (*For a list of CVEs released by Microsoft for September 2021 by the Zero Day Initiative click here.*)

References

Apple Releases Security Updates for Multiple Products *(To read click here)*

Attacks Targeting OMIGOD Vulnerability Ramping Up *(To read click here)*

Analyzing attacks that exploit the CVE-2021-40444 MSHTML vulnerability *(To read click here)*

Big Office bug squashed for September 2021's Patch Tuesday *(To read click here)*

BrakTooth: Impacts, Implications, and Next Steps *(To read click here)*

Cisco Releases Security Updates for Multiple Products *(To read click here)*

Citrix Releases Security Updates for Hypervisor *(To read click here)*

Critical encryption vulnerability found in secure communications platform Matrix *(To read click here)*

Close to half of on-prem databases contain vulnerabilities, with many critical flaws *(To read click here)*

Cisco fixes highly critical vulnerabilities in IOS XE Software *(To read click here)*

Exploitation of the CVE-2021-40444 vulnerability in MSHTML *(To read click here)*

Google Releases Security Updates for Chrome *(To read click here)*

Google Releases Security Updates for Chrome *(To read click here)*

How to fix printers asking for admins creds after PrintNightmare patch *(To read click here)*

Microsoft CVE Summary *(To read click here)*

Microsoft Patch Tuesday for Sept. 2021 — Snort rules and prominent vulnerabilities *(To read click here)*

Microsoft fixes remaining Windows PrintNightmare vulnerabilities *(To read click here)*

Microsoft patches Office zero-day in today's Patch Tuesday *(To read click here)*

Microsoft Patch Tuesday, September 2021 Edition *(To read click here)*

Microsoft patches 66 vulnerabilities in September update *(To read click here)*

Microsoft Patches Actively Exploited Windows Zero-Day Bug *(To read click here)*

Microsoft: Windows MSHTML bug now exploited by ransomware gangs *(To read click here)*

Microsoft asks Azure Linux admins to manually patch OMIGOD bugs *(To read click here)*

Microsoft September 2021 Patch Tuesday fixes 2 zero-days, 60 flaws *(To read click here)*

Microsoft September 2021 Patch Tuesday: Remote code execution flaws in MSHTML, OMI fixed *(To read click here)*

Microsoft shares temp fix for ongoing Office 365 zero-day attacks *(To read click here)*

Mozilla Releases Security Updates for Firefox, Firefox ESR, and Thunderbird *(To read click here)*

OMIGOD: Azure users running Linux VMs need to update now *(To read click here)*

OMIGOD: Microsoft Azure VMs exploited to drop Mirai, miners *(To read click here)*

Patch now! PrintNightmare over, MSHTML fixed, a new horror appears … OMIGOD *(To read click here)*

SonicWall fixes critical bug allowing SMA 100 device takeover *(To read click here)*

TangleBot: New Advanced SMS Malware Targets Mobile Users Across U.S. and Canada with COVID-19 Lures *(To read click here)*

THE SEPTEMBER 2021 SECURITY UPDATE REVIEW *(To read click here)*

Threat Brief: OMI Vulnerabilities (CVE-2021-38645, CVE-2021-38647, CVE-2021-38648 and CVE-2021-38649) *(To read click here)*

Week in review: The state of maritime cybersecurity, zero trust architecture challenges *(To read click here)*

WordPress Releases Security Update *(To read article here)*

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