SEPTEMBER 2020 - VULNERABILITIES OF INTEREST TO THE HEALTH SECTOR

Executive Summary

In September, 2020, a significant number of vulnerabilities in common information systems relevant to the healthcare sector have been disclosed to the public. This includes the Patch Tuesday vulnerabilities – released by several vendors on the second Tuesday of each month – as well as ad-hoc vulnerability announcements including mitigation steps and/or patches as they are developed. Vulnerabilities this month are from Microsoft, Adobe, Intel, SAP, Cisco, Apple, and Google. These vulnerabilities should be carefully considered for patching by any healthcare organization with special consideration to each vulnerability criticality category against the risk management posture of the organization.

MICROSOFT

On Tuesday, September 8, Microsoft announced 129 vulnerabilities, tied with June 2020 as the largest number of Patch Tuesday fixes ever. These 129 vulnerabilities 15 products and include 3 critical, 105 important, 1 moderate and no zero days, but a total of 32 remote code execution, 20 of which were classified critical. There are three noteworthy vulnerabilities:

1. Microsoft Exchange Memory Corruption Vulnerability (CVE-2020-16875) – This vulnerability allows for remote code execution by sending a crafted email to Exchange server. It has a CVSS score of 8.2.

2. Remote Code Execution Vulnerability for Microsoft COM for Windows (CVE-2020-0922), can be exploited by luring a user to a site with malicious JavaScript. It has a CVSS score of 7.9.

3. Remote Code Execution Vulnerability in Windows Text Service Module (CVE-2020-0908) - can be exploited by tricking a user to visiting a site with malicious code. It has a CVSS score of 6.7.

None of these vulnerabilities were known to have been exploited in the wild at the time of their publication.

Outside of the Patch Tuesday cycle, there became a public exploit available for CVE-2020-1472, also known as Zerologon was rated critical severity as it allows unauthenticated administrative access to a Windows domain controller (DC) and possible compromise of the entire domain and all resources it contains. Microsoft Windows domain controllers contain a flaw in a cryptographic authentication scheme (AES-CFB8) used by the Netlogon Remote Protocol allowing an attacker with only user-level access to gain administrative access. This would provide the attacker with additional opportunities including the creation of accounts for persistence as well as the compromise data on the network and the disruption of functionality of connected systems potentially impacting patient care. Microsoft released first phase update CVE-2020-1472 on August 11, 2020, with the second phase planned for February 9, 2021. The first phase enforces secure Remote ProtoCol (RPC) usage for machine accounts on Windows based devices, trust accounts and all Windows and non-Windows DCs. Within the new update, a new group policy is available as well as a secure registry key.

CVE2020-1472 affects multiple versions of Windows Server from 2008 to 2019. HC3 released a separate product on Zerologon which can be found at our website,

ADOBE

Adobe released 18 critical vulnerabilities as part of the September 2020 Patch Tuesday security updates for Adobe InDesign, Framemaker and Experience Manager, addressing multiple vulnerabilities.

INTEL

Intel released four patches (**INTEL-SA-00404**) for the Driver & Support Assistant, BIOS firmware for several of their platforms, Active Management Technology (AMT) and Intel Standard Manageability (ISM). The AMT and ISM are the most important as they are privilege escalation vulnerabilities both rated critical. Intel's latest security center advisories can always be found **here**.

SAP

SAP released 10 security advisories and updates to six previously released ones on September Patch Tuesday. This includes their Solution Manager, NetWeaver, and a number of other platforms that likely have minimal impact the healthcare industry. Their advisories can always be found by logging into their support portal.

ORACLE

Oracle releases patches on a quarterly basis. Their most recent release was their 2020 Q2 bulletin which was released in July and can be found here. Their next scheduled release will be Q3 (October).

CISCO

Cisco released 61 security advisories in the month of September including 1 critical, 36 high and 24 medium priority. Two vulnerabilities (CVE-2020-3421 and CVE-2020-3480) are in Cisco's Zone-Based Firewall, which according to the company, "could allow an unauthenticated, remote attacker to cause the device to reload or stop forwarding traffic through the firewall." There are also a number of vulnerabilities that are exploitable remotely, some not requiring authentication.

APPLE

Apple released updates their most recent security updates and iOS 14.0.1 in late September. This includes iCloud updates as well as macOS Sierra 10.13.6, Mojave 10.14.6 and Catalina 10.15.6 security updates.

GOOGLE

Google began releasing Android 11 in early September. On September 8th, they also released their monthly Android Security Bulletin, which included 52 vulnerabilities, 8 of which are rated critical.

REFERENCES

Microsoft September 2020 Security Updates
https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-Sep

Windows 10 Cumulative Updates KB4571756 & KB4574727 Released
https://www.bleepingcomputer.com/news/microsoft/windows-10-cumulative-updates-kb4571756-and-kb4574727-released/

Microsoft September 2020 Patch Tuesday
https://isc.sans.edu/forums/diary/Microsoft+September+2020+Patch+Tuesday/26544/

Microsoft Fixes 129 Vulnerabilities for September's Patch Tuesday
https://www.darkreading.com/vulnerabilities---threats/microsoft-fixes-129-vulnerabilities-for-septembers-patch-tuesday/d/d-id/1338863

Adobe fixes critical vulnerabilities in InDesign and Framemaker
https://www.bleepingcomputer.com/news/security/adobe-fixes-critical-vulnerabilities-in-indesign-and-framemaker/

Adobe Security Bulletins Posted
https://blogs.adobe.com/psirt/?p=1916

Google releases Android 11 with new features and privacy enhancements
https://www.zdnet.com/article/google-releases-android-11-with-new-features-and-privacy-enhancements/

Windows 10 starts bundling servicing stack updates with cumulative updates
https://www.bleepingcomputer.com/news/microsoft/windows-10-starts-bundling-servicing-stack-updates-with-cumulative-updates/

Android 11 system update from Google adds privacy controls
https://www.bbc.com/news/technology-54078019

Intel® Product Security Center Advisories
https://www.intel.com/content/www/us/en/security-center/default.html

Security update deployment information: September 8, 2020
https://support.microsoft.com/en-us/help/20200908/security-update-deployment-information-september-8-2020

Critical Adobe Flaws Allow Attackers to Run JavaScript in Browsers
https://threatpost.com/critical-adobe-flaws-attackers-javascript-browsers/159026/

Microsoft addresses 129 security vulnerabilities in its September 2020 Patch Tuesday update
https://www.computing.co.uk/news/4019912/microsoft-addresses-129-security-vulnerabilities-september-2020-patch-tuesday-update

Microsoft Releases September 2020 Security Patches For 129 Flaws
https://thehackernews.com/2020/09/patch-tuesday-september.html

Microsoft Patches 129 CVEs in Another Major Monthly Update
https://www.infosecurity-magazine.com/news/microsoft-patches-129-cves-monthly/

September 2020 Patch Tuesday: Microsoft fixes over 110 CVEs again
https://www.helpnetsecurity.com/2020/09/08/september-2020-patch-tuesday/

Critical Adobe Flaws Allow Attackers to Run JavaScript in Browsers
https://threatpost.com/critical-adobe-flaws-attackers-javascript-browsers/159026/

Microsoft Patch Tuesday, Sept. 2020 Edition
https://krebsonsecurity.com/2020/09/microsoft-patch-tuesday-sept-2020-edition/

Patch Wednesday fixes 'worst-case scenario' Exchange bug
https://www.itnews.com.au/news/patch-wednesday-fixes-worst-case-scenario-exchange-bug-553009

Microsoft addresses critical SharePoint and DNS-related flaws in Patch Tuesday update
https://portswigger.net/daily-swig/microsoft-addresses-critical-sharepoint-and-dns-related-flaws-in-patch-tuesday-update

September Patch Tuesday Updates Exchange, SharePoint
https://www.trendmicro.com/en_us/research/20/i/september-patch-tuesday-updates-sharepoint-gaps.html

Microsoft Office September security updates fix critical RCE bugs
https://www.bleepingcomputer.com/news/security/microsoft-office-september-security-updates-fix-critical-rce-bugs/

Critical Intel Active Management Technology Flaw Allows Privilege Escalation
https://threatpost.com/critical-intel-active-management-technology-flaw-allows-privilege-escalation/159036/

Microsoft's 'Patch Tuesday' Contains 129 Safety Updates, Principally to Home windows
https://www.editorials360.com/2020/09/12/microsofts-patch-tuesday-contains-129-safety-updates-principally-to-home-windows/

CVE-2020-16875
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16875

CVE-2020-0922
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0922

CVE-2020-0908
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0908

CVE-2020-1472
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1472

CVE-2020-3421
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3421

CVE-2020-3480
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3480

Android 11
https://developer.android.com/about/versions/11

Cisco Patch-Palooza Tackles 29 High-Severity Bugs
https://threatpost.com/cisco-patches-bugs/159537/

Google Android Security Bulletin – September 2020
https://source.android.com/security/bulletin/2020-09-01