NOVEMBER 2020 - VULNERABILITIES OF INTEREST TO THE HEALTH SECTOR

In November 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 MobileIron. 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

Microsoft released 112 patches, 18 of which have been classified as critical by Microsoft, with another 92 as important, 2 moderate and one zero-day. Of these, 24 are remote code execution (RCE) vulnerabilities meaning that when executed, the attacker can execute malicious code on the victim system, potentially giving them total control over it. The RCE vulnerabilities affecting applications and protocols utilized across many industries, including healthcare, such as Excel, SharePoint, Exchange Server, Network File System, the Windows GDI+ component, the Windows printing spooler service, and Microsoft Teams. One of the critical vulnerabilities has already reportedly been compromised in the wild. The zero-day (CVE-2020-17087) was disclosed at the end of October 30 by Google. Attackers would use the Chrome zero-day to run malicious code inside Chrome and then use the Windows zero-day to escape the Chrome security sandbox and elevate the code's privileges to attack the underlying OS. the zero-day resides in the Windows kernel's cryptography driver (cng.sys) and impacts all currently supported versions of the Windows OS. This includes all versions after Windows 7, and all Windows Server distributions. These vulnerabilities apply to platforms utilized in the healthcare industry and have the potential to impact healthcare industry information infrastructure. Also of note, Microsoft released non-security (functional) updates for windows in early November which are tracked as KB4586786 and KB4586781.

ADOBE

Adobe released security update APSB20-67, APSB20-69 and ASPB20-71. The first addresses vulnerabilities in Adobe Acrobat and Reader, three of which are remote code execution vulnerabilities and rated critical. The second addresses vulnerabilities in Adobe Connect (versions 11 and earlier) and includes one arbitrary browser JavaScript execution vulnerability rated important. The third addresses Adobe Reader Mobile (20.6 and earlier versions) and is an information disclosure vulnerability rated important. These vulnerabilities apply to platforms utilized in the healthcare industry and have the potential to impact healthcare industry information infrastructure.

INTEL

Intel **released 95 patches in 40 security advisories in November**. One of the vulnerabilities (**CVE-2020-8752)** was rated critical with a CVSS score of 9.4/10 in the Intel Active Management Technology (AMT) and Intel Standard Manageability (ISM) products. This is an out-of-bounds write in the IPv6 subsystem of Intel AMT and ISM (versions prior to 11.8.80, 11.12.80, 11.22.80, 12.0.70, 14.0.45) that enables remote unauthenticated to escalate privileges. Also, Microsoft **released Intel microcode updates** for Windows

1020H2, 2004, 1909, and older versions to fix new vulnerabilities discovered in Intel CPUs (including **PLATYPUS**). It's worth noting that previous updates have caused system and performance issues on older CPUs due to complications with specific vulnerability mitigations. HC3 recommends deploying updates in a test environment before applying them to operational systems.

SAP

SAP released 12 security advisories and updates to three previously released ones on November Patch Tuesday. This includes two vulnerabilities with a 10 CVSS rating, four of them with a 9+ CVSS and three more rated at 7.5, 7.5 and 8.6. These vulnerabilities are in platforms such as the SAP solution manager, SAP Data Services, NetWeaver and Commerce Cloud. Vulnerabilities vary from missing authentication checks to code injection to privilege escalation to cross-site scripting. Any healthcare organization whose information infrastructure includes SAP platforms is strongly encouraged to review these advisories for applicability. SAP advisories can always be found by logging into their support portal.

ORACLE

Oracle releases patches on a quarterly basis. Their last release – 2020 Q4 – was in October and the next is expected in January 2021. Oracle did release a security alert related to a remote code execution vulnerability (CVE-2020-14750) in their WebLogic Server versions 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Oracle technology is widely utilized by the healthcare industry and therefore these patches should be carefully reviewed and implemented as appropriate.

CISCO

Cisco released 59 vulnerability patches in November. Four of them are rated critical and are as follows:

1. Cisco Security Manager Path Traversal Vulnerability – CVSS score of 9.1, CVE-2020-27130
2. Cisco IoT Field Network Director Unauthenticated REST API Vulnerability – CVSS score 9.8, CVE-2020-3531
3. Cisco DNA Spaces Connector Command Injection Vulnerability – CVSS score 9.4, CVE-2020-3586
4. Cisco Integrated Management Controller Multiple Remote Code Execution Vulnerabilities – CVSS score 9.8, CVE-2020-3470

The four above vulnerabilities should be prioritized. Furthermore, eighteen of the vulnerabilities were categorized as high and involved several important applications and platforms, such as SD-WAN, Webex, Security Manager and IoT Field Network Director. These should also be reviewed for applicability.

APPLE

Apple released security updates including three zero-day vulnerabilities for iCloud, iOS, macOS, iTunes, Safari, watchOS and iTunes. While these products generally don't apply directly to the health sector specifically, many of them would potentially expand the attack surface of a healthcare organization as part of a bring-your-own-device program or, as health-monitoring devices, expose PII/PHI related information to potential data breaches.

MobileIron

MobileIron released several patches in November, most notably a remote code execution flaw in its Core and Connector platforms (CVE-2020-15505) with a CVSS score of 9.8 and should be patched immediately.

REFERENCES

Windows Kernel Local Elevation of Privilege Vulnerability
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-17087

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

November Patch Tuesday fixes close 112 holes—including one already being exploited
https://news.sophos.com/en-us/2020/11/10/november-patch-tuesday-fixes-close-112-holes-including-one-already-being-exploited/

Issue 2104: Windows Kernel cng.sys pool-based buffer overflow in IOCTL 0x390400
https://bugs.chromium.org/p/project-zero/issues/detail?id=2104

Microsoft November 2020 Patch Tuesday arrives with fix for Windows zero-day
https://www.zdnet.com/article/microsoft-november-2020-patch-tuesday-arrives-with-fix-for-windows-zero-day/

Microsoft November 2020 Patch Tuesday fixes 112 vulnerabilities
https://www.bleepingcomputer.com/news/security/microsoft-november-2020-patch-tuesday-fixes-112-vulnerabilities/

November 10, 2020—KB4586786 (OS Builds 18362.1198 and 18363.1198)
https://support.microsoft.com/en-us/help/4586786/windows-10-update-kb4586786

Microsoft November 2020 Patch Tuesday fixes 112 vulnerabilities
https://www.bleepingcomputer.com/news/security/microsoft-november-2020-patch-tuesday-fixes-112-vulnerabilities/

November 10, 2020—KB4586781 (OS Builds 19041.630 and 19042.630)
https://support.microsoft.com/en-us/help/4586781/windows-10-update-kb4586781

Windows 10 Cumulative Updates KB4586786 & KB4586781 Released
https://www.bleepingcomputer.com/news/microsoft/windows-10-cumulative-updates-kb4586786-and-kb4586781-released/

November 2020 Patch Tuesday: Microsoft fixes actively exploited Windows Kernel flaw
https://www.helpnetsecurity.com/2020/11/10/november-2020-patch-tuesday/

Microsoft November 2020 Patch Tuesday arrives with fix for Windows zero-day
https://www.zdnet.com/article/microsoft-november-2020-patch-tuesday-arrives-with-fix-for-windows-zero-day/
Microsoft November 2020 Patch Tuesday
https://isc.sans.edu/forums/diary/Microsoft+November+2020+Patch+Tuesday/26778/

November Patch Tuesday Fixes Exchange, NFS Vulns
https://www.trendmicro.com/en_us/research/20/k/november-patch-tuesday-fixes-exchange-nfs-vulns.html

Microsoft Patch Tuesday Update Fixes 17 Critical Bugs
https://threatpost.com/microsoft-patch-tuesday-critical-bugs/161098/

Microsoft Patch Tuesday for Nov. 2020 — Snort rules and prominent vulnerabilities
https://blog.talosintelligence.com/2020/11/microsoft-patch-tuesday-for-nov-2020.html

Office November security updates fix remote code execution bugs
https://www.bleepingcomputer.com/news/security/office-november-security-updates-fix-remote-code-execution-bugs/

Patch Tuesday: Microsoft addresses Windows zero-day vulnerability and 111 others
https://www.computing.co.uk/news/4023093/patch-tuesday-microsoft-addresses-windows-zero-day-vulnerability-111

Bulletin (SB20-314) Vulnerability Summary for the Week of November 2, 2020
https://us-cert.cisa.gov/ncas/bulletins/sb20-314

Bulletin (SB20-321) Vulnerability Summary for the Week of November 9, 2020
https://us-cert.cisa.gov/ncas/bulletins/sb20-321

Bulletin (SB20-328) Vulnerability Summary for the Week of November 16, 2020
https://us-cert.cisa.gov/ncas/bulletins/sb20-328

Bulletin (SB20-335) Vulnerability Summary for the Week of November 23, 2020
https://us-cert.cisa.gov/ncas/bulletins/sb20-335

Adobe releases security update for Adobe Reader for Android
https://www.bleepingcomputer.com/news/security/adobe-releases-security-update-for-adobe-reader-for-android/

Security Updates Available for Adobe Acrobat and Reader | APSB20-67
https://helpx.adobe.com/security/products/acrobat/apsb20-67.html

Adobe: Security updates available for Adobe Connect | APSB20-69
https://helpx.adobe.com/security/products/connect/apsb20-69.html

Security update available for Adobe Reader Mobile | APSB20-71
https://helpx.adobe.com/security/products/reader-mobile/apsb20-71.html

Vulnerability Spotlight: Multiple JavaScript vulnerabilities in Adobe Acrobat Reader
https://blog.talosintelligence.com/2020/11/vulnerability-spotlight-multiple.html
Adobe Releases Security Updates for Multiple Products
https://us-cert.cisa.gov/ncas/current-activity/2020/11/10/adobe-releases-security-updates-multiple-products

Intel and AMD processors affected by another side-channel exploit
https://www.computerweekly.com/news/252491855/Intel-and-AMD-processors-affected-by-another-side-channel-exploit

Intel fixes 95 vulnerabilities in November 2020 Platform Update
https://www.bleepingcomputer.com/news/security/intel-fixes-95-vulnerabilities-in-november-2020-platform-update/

Windows 10 Intel microcode released to fix new CPU security bugs
https://www.bleepingcomputer.com/news/microsoft/windows-10-intel-microcode-released-to-fix-new-cpu-security-bugs/

CVE-2020-8752
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8752

SAP Security Patch Day – November 2020
https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=562725571

CVE-2020-14750
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14750

Oracle Security Alert Advisory - CVE-2020-14750
https://www.oracle.com/security-alerts/alert-cve-2020-14750.html

Oracle issues emergency patch for critical WebLogic Server flaw
https://www.bleepingcomputer.com/news/security/oracle-issues-emergency-patch-for-critical-weblogic-server-flaw/

Cisco Security Manager Path Traversal Vulnerability
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-csm-path-trav-NgeRnqgR

CVE-2020-27130
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27130

Cisco IoT Field Network Director Unauthenticated REST API Vulnerability
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-FND-BCK-GHkPNZ5F

CVE-2020-3531
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2020-3531

CVE-2020-3586
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3586

Cisco DNA Spaces Connector Command Injection Vulnerability
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dna-cmd-injection-rrAYzOwc

CVE-2020-3470
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3470

Cisco Integrated Management Controller Multiple Remote Code Execution Vulnerabilities
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucs-api-rce-UXwpeDHd

Cisco Releases Security Updates for Multiple Products
https://us-cert.cisa.gov/ncas/current-activity/2020/11/19/cisco-releases-security-updates-multiple-products

High-Severity Cisco DoS Flaw Can Immobilize ASR Routers
https://threatpost.com/high-severity-cisco-dos-flaw-asr-routers/161115/

Cisco Releases Security Update for IOS XR Software
https://us-cert.cisa.gov/ncas/current-activity/2020/11/10/cisco-releases-security-update-ios-xr-software

Apple Patches 24 Vulnerabilities Across Product Lines
https://www.darkreading.com/vulnerabilities---threats/apple-patches-24-vulnerabilities-across-product-lines/d/d-id/1339399

Apple Releases Security Updates for Multiple Products
https://us-cert.cisa.gov/ncas/current-activity/2020/11/06/apple-releases-security-updates-multiple-products

CVE-2020-15505
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15505

MobileIron Security Updates Available
https://www.mobileiron.com/en/blog/mobileiron-security-updates-available