Health Sector Cybersecurity Coordination Center (HC3)

Monthly Cybersecurity Vulnerability Bulletin

October 2020

OCTOBER 2020 - VULNERABILITIES OF INTEREST TO THE HEALTH SECTOR

In October, 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

For October 2020 Patch Tuesday, Microsoft released 87 patches, 12 were classified as critical, 74 important and 1 moderate and there were no zero days (previously unknown vulnerabilities). Six of these were previously publicly disclosed. One of the most egregious of these is a remote code execution vulnerability (CVE-2020-16898) in the Windows TCP/IP stack that improperly handles ICMPv6. To exploit this vulnerability, an attacker would have to send a specially crafted Router Advertisement packet to a vulnerable system. The patch corrects how the system's TCP/IP stack handles ICMPv6 Router Advertisement packets. There were four other critical remote code execution (RCE) vulnerabilities of note. One is with Microsoft Outlook and can allow attackers to execute commands by sending a specially crafted e-mail which the victim needs to open to be exploited. One is in the graphics device interface, another with Hyper-V – what windows uses for hardware virtualization, and a media foundation memory corruption vulnerability that can provide remote code exploitation if targeted. There's also an exploit in the remote desktop protocol (RDP) (CVE-2020-16896) which allows for information disclosure when compromised and therefore potentially allows for an attacker to collect system information for reconnaissance purposes to enable a follow-on attack. These vulnerabilities apply to platforms utilized in the healthcare industry and have the potential to impact healthcare industry information infrastructure.

ADOBE

Adobe released security update APSB20-58 which addresses a critical (priority 2) remote code execution vulnerability in Adobe Flash Player (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200012). Adobe Flash is a common application contained in the infrastructure of many industries, including healthcare. It's worth noting that Adobe will be discontinuing Flash by the end of the year. Nonetheless, this vulnerability should still be addressed as a priority.

INTEL

Intel released a single patch related to the BlueZ open-source Bluetooth stack, tracked as INTEL-SA-00435. This is not believed to have a significant impact on the healthcare sector, however, appropriate implementation as needed is recommended.

SAP

SAP released 15 security advisories and updates to six previously released ones on October Patch Tuesday. This includes an OS Command Injection vulnerability in SAPs CA Introscope Enterprise Manager. This is not believed to have a significant impact on the healthcare sector, however, appropriate implementation as needed is recommended. Their advisories can always be found by logging into their support portal.

ORACLE

Oracle releases patches on a quarterly basis. They released their 2020 Q4 updates in October, which included 402 patches for 28 of their product sets. This was double the number of vulnerabilities from the same time last year and it includes Oracle Big Data Graph, REST Data Services, TimesTen In-Memory Database, Communications Apps, Enterprise Risk Manager, and Financial Services Apps. The majority of the patchers are in Oracle Financial Services Applications (53), Oracle MySQL (53), Oracle Communications (52), Oracle Fusion Middleware (46), Oracle Retail Applications (28) and Oracle E-Business Suite (27).

Over half of the flaws in Oracle's quarterly patch update can be remotely exploitable without authentication; two have CVSS scores of 10 out of 10. This includes a vulnerability (CVE-2020-1953) in the self-service analytics component of Oracle Healthcare Foundation, which is a unified healthcare-analytics platform that is part of the Oracle Health Science Applications suite. This can be remotely exploited without requiring any user credentials, requires no user interaction and is trivial to exploit. Impacted versions include 7.1.1, 7.2.0, 7.2.1 and 7.3.0.The second severe flaw (CVE-2020-14871) exists in the pluggable authentication module of versions 10 and 11 of Oracle Solaris, its enterprise operating system for Oracle Database and Java applications, and is also remotely exploitable without user credentials, requires no user interaction and is also a trivial attack. Sixty-five have a CVSS rating of 9.8 of 10 and 272 of them can be remotely exploited without user credentials including all the Java SE vulnerabilities and most of the Oracle E-Business Suite, PeopleSoft, and Fusion Middleware vulnerabilities.

Oracle technology is widely utilized by the healthcare industry and therefore these patches should be carefully reviewed and implemented as appropriate. Users running Java SE with a browser can download the latest release from http://java.com and those with the Windows and Mac OS X platforms can also use automatic updates to get the latest release.

CISCO

Cisco released a number of vulnerability patches in October (ERP-74302) impacting their Adaptive Security Appliance (ASA), Firepower Threat Defense (FTD), and Firepower Management Center (FMC) products. A majority of these can be exploited remotely without authentication, including the modification of data via a man-in-the-middle attack, user spoofing, and bypassing FMC authentication. Many of the vulnerabilities that allow for remote exploitation without authentication cause a denial-of-service (DoS) condition and in some cases, recovering from this DoS condition requires a reboot of the device.

APPLE

Apple released security updates for macOS and watchOS, among other products. 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.

GOOGLE

Google release a series of security updates in early October which can be found on their security advisories page. These 51 vulnerabilities across the month, primarily categorized as medium impact with some of them ranked high and none considered critical. The potential effects of exploitation of these vulnerabilities include denial of service, authorization bypass and arbitrary code execution. They should be prioritized and patched as applicable by any healthcare organization that employs Cisco technology in their enterprise infrastructure.

National Security Agency

The National Security Agency released a bulletin on the top 25 vulnerabilities exploited by Chinese state-sponsored malicious cyber actors. Because of historic targeting of healthcare organizations by China as well as the applicability of the 25 vulnerabilities in the alert to the healthcare industry, HHS recommends review of this bulletin and patching/mitigation of any applicable vulnerabilities. Many of the types of technologies, such as VNPs, application delivery controllers, mobile device managers and messaging technologies are common in the healthcare industry.

REFERENCES

Microsoft October 2020 Patch Tuesday fixes 87 security bugs
https://www.bleepingcomputer.com/news/security/microsoft-october-2020-patch-tuesday-fixes-87-security-bugs/

Chrome 86 rolls out with massive user security enhancements
https://www.bleepingcomputer.com/news/google/chrome-86-rolls-out-with-massive-user-security-enhancements/

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

CVE-2020-16898
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16898

CVE-2020-16896
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16896

ADV200012 | October 2020 Adobe Flash Security Update
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200012

Adobe fixes critical security vulnerability in Flash Player
https://www.bleepingcomputer.com/news/security/adobe-fixes-critical-security-vulnerability-in-flash-player/

APSB20-58
https://helpx.adobe.com/security/products/flash-player/apsb20-58.html

INTEL-SA-00435
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00435.html

IPAS: SECURITY ADVISORIES FOR OCTOBER 2020
https://blogs.intel.com/technology/2020/10/ipas-security-advisories-for-october-2020/#gs.k0bf2e

SAP Security Patch Day – October 2020
https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=558632196

SAP Releases October 2020 Security Updates
https://us-cert.cisa.gov/ncas/current-activity/2020/10/13/sap-releases-october-2020-security-updates

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

Oracle Critical Patch Update Advisory - October 2020
https://www.oracle.com/security-alerts/cpuoct2020.html

CVE-2020-1953
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1953

CVE-2020-14871
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14871

Cisco ERP-74302
https://tools.cisco.com/security/center/viewErp.x?alertId=ERP-74302

Chinese State-Sponsored Actors Exploit Publicly Known Vulnerabilities
https://media.defense.gov/2020/Oct/20/2002519884/-1/-1/0/CSA_CHINESE_EXPLOIT_VULNERABILITIES_U00179811.PDF