Health Sector Cybersecurity Coordination Center (HC3)
Monthly Cybersecurity Vulnerability Bulletin
January 12, 2021 **TLP: White** **Report: 202101120900**

DECEMBER 2020 - VULNERABILITIES OF INTEREST TO THE HEALTH SECTOR

In December, 2020, a number of vulnerabilities in common information systems relevant to the healthcare sector have been disclosed to the public however the ones that were released warrant attention. 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 58 patches, 22 of which are remote code execution (RCE) vulnerabilities which allow an attacker significant control over a compromised system. Of these 9 are classified as critical, 46 are important and 3 are important. None are known to have been exploited prior to disclosure by Microsoft. Some of the more egregious and likely to impact healthcare organizations are:

1. CVE-2020-16996 – Kerberos Security Feature Bypass Vulnerability
2. CVE-2020-17099 – Windows Lock Screen Security Feature Bypass Vulnerability
3. CVE-2020-17132 – Microsoft Exchange Remote Code Execution Vulnerability
4. CVE-2020-17121 – Microsoft SharePoint Remote Code Execution Vulnerability
5. CVE-2020-17095 – Hyper-V Remote Code Execution Vulnerability
6. CVE-2020-17118 – Microsoft SharePoint Remote Code Execution Vulnerability
7. CVE-2020-17096 – Windows NTFS Remote Code Execution Vulnerability

The full list can be found at Microsoft's Security Update Guide.

ADOBE

Adobe released security updates for the following products APSB20-75 (Adobe Acrobat and Reader), APSB20-74 (Adobe Lightroom), APSB20-72 (Adobe Experience Manager) and APSB20-70 (Adobe Prelude). Most importantly, Adobe Flash reached its official end-of-life and will no longer be supported with security updates. Adobe recommends uninstalling all instances of Flash as soon as practical. Adobe vulnerabilities can be found on their Security Bulletins and Advisories page.

INTEL

Intel released just **eleven updates**. These are primarily firmware and driver updates and none of them are especially egregious, they should be implemented in a timely manner. Intel's full list of security updates can be found **here**.

SAP

SAP released 11 security advisories which include four with a CVSS score of at least a 9. Two of those are code injection vulnerabilities affecting their business platforms as well as two authentication vulnerabilities, in its NetWeaver and Business Intelligence platforms. 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 released patches on a quarterly basis. Their last release – 2020 Q4 – was in October and the next is expected in January 2021. Oracle technology is widely utilized by the healthcare industry and therefore these patches should be carefully reviewed and implemented as appropriate.

CISCO

Cisco released 12 security advisories in December. One of them was categorized as critical – related to three vulnerabilities in Jabber Desktop and Mobile Client application. This is associated with the following vulnerabilities: CVE-2020-26085, CVE-2020-27127 and CVE-2020-27132.

APPLE

Apple released security updates most notable for iCloud, iOS, macOS Server, iTunes, Safari and watchOS. 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.

REFERENCES

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

Adobe APSB20-75 Security Bulletin
https://helpx.adobe.com/security/products/acrobat/apsb20-75.html

Adobe APSB20-74 Security Bulletin
https://helpx.adobe.com/security/products/lightroom/apsb20-74.html

Adobe APSB20-72Security Bulletin
https://helpx.adobe.com/security/products/experience-manager/apsb20-72.html

Adobe APSB20-70 Security Bulletin
https://helpx.adobe.com/security/products/prelude/apsb20-70.html

Intel December 2020 Security Updates
https://blogs.intel.com/technology/2019/12/ipas-security-advisories-for-december-2019/#gs.ptocw7

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