Vulnerabilities of Interest to the Health Sector

Executive Summary

In January 2021, a relatively small 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 and Apple. 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.

Report

Microsoft

For January 2021 Patch Tuesday, Microsoft released 83 patches, 10 of which are classified critical and one is a zero day. The zero day (one of the ten critical) is in their endpoint security software, Defender and it's a remote code execution vulnerability being tracked as CVE-2021-1647 and its being exploited in the wild. It's also known to be part of the SolarWinds compromise. Microsoft also patched a vulnerability in the Windows print driver process SPLOWOW64.exe. This is a privilege escalation vulnerability and it's tracked as CVE-2021-1648. There was another critical RCE vulnerability in the Edge browser, CVE-2021-1705. The full list can be found at Microsoft's Security Update Guide. This guide has recently changed and we recommend this article (free registration required) to review those changes. Microsoft also released a security update to address multiple vulnerabilities in its Chromium-based Edge browser. Upon exploitation, an attacker could take control of an affected system. This is described in further detail in Microsoft Security Advisory ADV200002.

Adobe

In the month of January, released patches for vulnerabilities in many of their graphics platforms as well as other applications. While the functionality of these software systems may not be critical to healthcare operations, exploitation of vulnerabilities in them may present an attacker with the opportunity to leverage additional follow-up attacks towards further compromise of their enterprise infrastructure, potentially creating a significant impact on operations. These vulnerabilities include the following:

- Photoshop (APSB21-01)
- Illustrator (ASPB21-02)
- Animate (ASPB21-03)
- Campaign Classic (APSB21-04)

- InCopy (APSB21-05)
- Captivate (APSB21-06)
- Bridge (APSB21-07)

Adobe vulnerabilities can be found on their Security Bulletins and Advisories page.

Intel

In January, Intel released **six updates**. These are entirely software updates (as opposed to the more typical firmware/hardware updates). These are as follows:

Security Advisory ID	Title	CVEs	CVSS
INTEL-SA-00325	Intel VTUNE Advisory	**CVE-2019-14613**	8.2
INTEL-SA-00308	Intel RWC 3 for Windows* Advisory	**CVE-2019-14601**	6.7
INTEL-SA-00300	Intel SNMP Subagent Stand-Alone for Windows Advisory	**CVE-2019-14600**	6.5
INTEL-SA-00314	Intel Processor Graphics Advisory	**CVE-2019-14615**	6.3
INTEL-SA-00306	Intel Chipset Device Software INF Utility Advisory	**CVE-2019-14596**	5.9
INTEL-SA-00332	Intel DAAL Advisory	**CVE-2019-14629**	3.9

Intel's full list of security updates can be found **here**.

SAP

SAP released 6 security advisories. One was a cross-site scripting vulnerability in the Rest Adapter of their Process Integration platform and another was a denial-of-service vulnerability in their NetWeaver Internet Communication Manager. 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. In January, they released their 2021 Q1 Critical Patch Update Advisory which included 329 patches for more than 20 products and third-party components included in their products. Fusion Middleware was their platform most affected with 60 patches, 47 which were remotely exploitable and did not require authentication. Financial Services Applications were the second most affected, with 50 patches, of which 41 are remotely-exploitable. MySQL received 43 patches, and 5 of those were remotely exploitable and did not require authentication. Fourth was Retail Applications, which saw 32 patches, each remotely

exploitable without authentication. Fifth was E-Business Suite, with 31 patches, each remotely exploitable without authentication. Other patched Oracle platforms are as follows:

- Virtualization (17 patches)
- Communications (12 patches)
- Enterprise Manager (8 patches)
- PeopleSoft (8 patches)
- Communications Applications (8 patches)
- Construction and Engineering (7 patches)
- Hyperion (7 patches)
- JD Edwards (5 patches)
- Health Sciences Applications (5 patches)
- Systems (4 patches)
- Siebel CRM (4 patches)
- Insurance Applications (3 patches)
- GraalVM (2 patches)
- Food and Beverage Applications (2 patches)
- Java SE (1 patch)
- Utilities Applications (1 patch)

This release includes fixes for CVE-2020-14750, an exploited vulnerability in WebLogic Server. Oracle's next Critical Patch Update Advisory is expected in April 20, 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 67 security advisories in January, four of which were classified as critical. The four critical are as follows:

Remote Command Execution and Denial of Service vulnerabilities for RV110W, RV130, RV130W, and RV215W Routers.
Command Injection Vulnerabilities for Smart Software Manager Satellite Web UI
Command Injection Vulnerability for Cisco DNA Center Command Runner
Buffer Overflow Vulnerabilities in SD-WAN

There were also thirteen vulnerabilities categorized as high which should be reviewed and addressed as a priority.

Apple

Apple released security updates most notable for iCloud, iOS, iPadOS, XCode, tvOS 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
- Microsoft Releases Security Updates for Edge
- https://us-cert.cisa.gov/ncas/current-activity/2021/01/11/microsoft-releases-security-updates-edge
- Google Releases Security Updates for Chrome
- https://us-cert.cisa.gov/ncas/current-activity/2021/01/07/google-releases-security-updates-chrome
- Mozilla Releases Security Updates for Firefox, Firefox for Android, and Firefox ESR
- https://us-cert.cisa.gov/ncas/current-activity/2021/01/07/mozilla-releases-security-updates-firefox-firefox-android-and
- MS-ISAC Releases Cybersecurity Advisory on Zyxel Firewall and AP Controllers
- https://us-cert.cisa.gov/ncas/current-activity/2021/01/08/ms-isac-releases-cybersecurity-advisory-zyxel-firewall-and-ap
- CISA Bulletin (SB21-011) Vulnerability Summary for the Week of January 4, 2021
- https://us-cert.cisa.gov/ncas/bulletins/sb21-011
- Mozilla Releases Security Update for Thunderbird
- https://us-cert.cisa.gov/ncas/current-activity/2021/01/12/mozilla-releases-security-update-thunderbird
- SAP Releases January 2021 Security Updates
- https://us-cert.cisa.gov/ncas/current-activity/2021/01/12/sap-releases-january-2021-security-updates
- Adobe Releases Security Updates for Multiple Products
- https://us-cert.cisa.gov/ncas/current-activity/2021/01/12/adobe-releases-security-updates-multiple-products
- Cisco Releases Security Updates for Multiple Products
- https://us-cert.cisa.gov/ncas/current-activity/2021/01/14/cisco-releases-security-updates-multiple-products
- RCE Vulnerability Affecting Microsoft Defender
- https://us-cert.cisa.gov/ncas/current-activity/2021/01/14/rce-vulnerability-affecting-microsoft-defender
- Juniper Networks Releases Security Updates for Multiple Products
- https://us-cert.cisa.gov/ncas/current-activity/2021/01/14/juniper-networks-releases-security-updates-multiple-products
- Apache Releases Security Advisory for Tomcat
- https://us-cert.cisa.gov/ncas/current-activity/2021/01/15/apache-releases-security-

advisory-tomcat

- Cisco Releases Advisories for Multiple Products
- https://us-cert.cisa.gov/ncas/current-activity/2021/01/21/cisco-releases-advisories-multiple-products
- Oracle Releases January 2021 Security Bulletin
- https://us-cert.cisa.gov/ncas/current-activity/2021/01/21/oracle-releases-january-2021-security-bulletin
- Oracle Critical Patch Update Advisory - January 2021
- https://www.oracle.com/security-alerts/cpujan2021.html
- CISA Bulletin (SB21-018) Vulnerability Summary for the Week of January 11, 2021
- https://us-cert.cisa.gov/ncas/bulletins/sb21-018
- Stable Channel Update for Desktop - Tuesday, January 19, 2021
- https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html
- Google Releases Security Updates for Chrome
- https://us-cert.cisa.gov/ncas/current-activity/2021/01/21/google-releases-security-updates-chrome
- Drupal releases fix for critical vulnerability with known exploits
- https://www.bleepingcomputer.com/news/security/drupal-releases-fix-for-critical-vulnerability-with-known-exploits/
- CISA Bulletin (SB21-025) Vulnerability Summary for the Week of January 18, 2021
- https://us-cert.cisa.gov/ncas/bulletins/sb21-025
- CVE-2021-1647
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1647
- Apple Releases Security Updates
- https://us-cert.cisa.gov/ncas/current-activity/2021/01/27/apple-releases-security-updates
- CVE-2021-1648
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1648
- CVE-2021-1705
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1705
- Critical Microsoft Defender Bug Actively Exploited; Patch Tuesday Offers 83 Fixes
- https://threatpost.com/critical-microsoft-defender-bug-exploited/162992/
- Microsoft fixes Defender zero-day in January 2021 Patch Tuesday
- https://www.zdnet.com/article/microsoft-fixes-defender-zero-day-in-january-2021-patch-tuesday/
- Microsoft January 2021 Patch Tuesday fixes 83 flaws, 1 zero-day
- https://www.bleepingcomputer.com/news/microsoft/microsoft-january-2021-patch-tuesday-fixes-83-flaws-1-zero-day/
- Microsoft Security Advisory ADV200002
- https://msrc.microsoft.com/update-guide/vulnerability/ADV200002
- CVE-2019-14600
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14600

- CVE-2019-14601
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14601
- CVE-2019-14613
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14613
- CVE-2019-14615
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=%20CVE-2019-14615
- CVE-2019-14596
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14596
- CVE-2019-14629
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14629
- CVE-2020-14750
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14750
- INTEL-SA-00325
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00325.html
- INTEL-SA-00308
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00308.html
- INTEL-SA-00300
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00300.html
- INTEL-SA-00314
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00314.html
- INTEL-SA-00306
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00306.html
- INTEL-SA-00332
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00332.html
- Oracle Critical Patch Update Advisory - January 2021
- https://www.oracle.com/security-alerts/cpujan2021.html
- Cisco Security Advisory: Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers Remote Command Execution and Denial of Service Vulnerabilities
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U

- Cisco Security Advisory: Cisco Smart Software Manager Satellite Web UI Command Injection Vulnerabilities
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-multici-pgG5WM5A
- Cisco Security Advisory: Cisco DNA Center Command Runner Command Injection Vulnerability
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-cmdinj-erumsWh9
- Cisco SD-WAN Buffer Overflow Vulnerabilities
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-bufovulns-B5NrSHbj