Vulnerabilities of Interest to the Health Sector

Executive Summary

In February, 2021, for a third month in a row, there were less than historic average 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 February 2021 Patch Tuesday, Microsoft released 53 patches, 11 of which are classified critical and one zero day. The zero day (one of the eleven critical) is a Windows Win32k Elevation of Privilege Vulnerability which has been exploited in the wild, is a local privilege escalation bug that affects several versions of Windows 10 and Windows Server. This vulnerability, CVE-2021-1732, is exploitable by attackers who either have local physical access, who can access it remotely, or who can induce a user into clicking a malicious link or opening a malicious document.

There were also multiple patches released by Microsoft regarding the Windows TCP/IP implementation, a set of fundamental networking protocols required for all Windows-based networks. These patches are related to the following vulnerabilities:

CVE-2021-24074 – This is a remote code execution vulnerability in Windows TCP/IP. This vulnerability is unique from CVE-2021-24094.
CVE-2021-24094 – This is a remote code execution vulnerability in Windows TCP/IP. This vulnerability affects Windows IPv6 deployments that are configured with IPv6 link-local addresses are not reachable by remote attackers. These addresses are not routable on the internet and therefore an attack would need to originate from the same logical or adjacent network segment.
CVE-2021-24086 – This is a Windows TCP/IP Denial of Service Vulnerability. This vulnerability affects Windows IPv6 deployments that are configured with IPv6 link-local addresses are not reachable by remote attackers. These addresses are not routable on the internet and therefore an attack would need to originate from the same logical or adjacent network segment.

The full list of Microsoft vulnerabilities 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.

ADOBE

In February, Adobe released security bulletin APSB21-09, which patches Acrobat and Reader applications. Special attention should be paid to CVE-2021-21017, a heap-based buffer overflow in Reader, which is being exploited in the wild. These patches should be tested and deployed as soon as possible. Adobe vulnerabilities can be found on their Security Bulletins and Advisories page.

INTEL

In February, Intel released **fifty-seven updates** as part of Patch Tuesday. Many of them are software driver updates for graphics components and firmware/software updates for networking components. Intel graphics driver vulnerabilities affect multiple processor generations up to the 10th generation and impact several versions of Windows and Linux drivers. The most egregious is **CVE-2020-0544**, which is an insufficient control flow management vulnerability that enables authenticated attackers to escalate privileges via local access. The issue is with the kernel mode driver for some Intel graphics drivers prior to version 15.36.39.5145. Intel's full archive of current and historic security updates can always be found **here**.

SAP

SAP released 7 security advisories. The three most important of these are note 2622660, which is related to the browser control Google Chromium delivered with SAP Business Client, note 3014121, which is a remote code execution vulnerability that impacts SAP Commerce versions 1808,1811,1905,2005,2011, and 2986980, which updates multiple vulnerabilities in the database interface for SAP Business Warehouse.

SAP advisories can always be found by logging into their support portal.

ORACLE

Oracle releases patches on a quarterly basis. In February, they released their 2021 Q1 Critical Patch Update Advisory included 329 patches for more than 20 products and third-party components as part of their products. The next release is expected in April.

CISCO

Cisco released 46 security advisories in February, five of which were classified as critical. The first is a series of virtual private network router remote code execution vulnerabilities (RV160, RV160W, RV260, RV260P, and RV260W). The second is a series of command injection vulnerabilities in their SD-WAN products which could allow the attacker to take actions with escalated privileges on the devices. Another is an unauthenticated arbitrary file actions vulnerability in Nexus 3000 Series Switches and Nexus 9000 Series Switches. There were also several vulnerabilities in the Cisco Application Services Engine which could allow an unauthenticated, remote attacker to gain privileged access, collect sensitive information, create files and make configuration changes. The fifth is an authentication bypass vulnerability in the API endpoint of Cisco ACI Multi-Site Orchestrator on the Application Services Engine which could allow

an unauthenticated, remote attacker unauthorized access to the device. There were also eighteen vulnerabilities categorized as high which should be reviewed and addressed as a priority.

APPLE

Apple released security updates most notably for macOS and Safari. 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

- Multiple Security Updates Affecting TCP/IP: CVE-2021-24074, CVE-2021-24094, and CVE-2021-24086
  https://msrc-blog.microsoft.com/2021/02/09/multiple-security-updates-affecting-tcp-ip/

- CVE-2021-24074
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24074

- CVE-2021-24094
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24094

- CVE-2021-24086
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24086

- Adobe Security Bulletin APSB21-09
  https://helpx.adobe.com/security/products/acrobat/apsb21-09.html

- CVE-2021-21017
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21017

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0544
  CVE-2020-0544

- SAP security note 2622660
  https://launchpad.support.sap.com/#/notes/2622660

- SAP security note 3014121
  https://launchpad.support.sap.com/#/notes/3014121

- SAP security note 2986980
  https://launchpad.support.sap.com/#/notes/2986980

- Cisco SD-WAN Command Injection Vulnerabilities
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn

- Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers Remote Code Execution Vulnerabilities
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf

- Cisco NX-OS Software Unauthenticated Arbitrary File Actions Vulnerability
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-3000-9000-fileaction-QtLzDRy2

- Cisco Application Services Engine Unauthorized Access Vulnerabilities
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-case-mvuln-dYrDPC6w

- Cisco ACI Multi-Site Orchestrator Application Services Engine Deployment Authentication Bypass Vulnerability
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-mso-authbyp-bb5GmBQv