LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF INFORMATION SECURITY

HC3: Monthly Cybersecurity Vulnerability Bulletin

April 2021 TLP: White Report: 202105071600

Vulnerabilities of Interest to the Health Sector

Executive Summary

In April 2021, there were numerous vulnerabilities in common information systems relevant to the healthcare sector that were 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, SAP, Cisco and Apple. These vulnerabilities should be triaged and prioritized for patching by healthcare organizations with special consideration to each vulnerability criticality category against the risk management posture of the enterprise.

MICROSOFT

Microsoft released 108 patches, about half of them allowing for remote code execution, 19 categorized as critical, five of them zero days, and one of the patches was actively exploited prior to discovery. Microsoft followed up it's patching of the Proxylogon vulnerability in its Exchange Server platform in early March with updates in April to fix four more flaws in Exchange Server versions 2013 through 2019. These were reportedly discovered by the National Security Agency and subsequently incorporated into supplemental direction for a Department of Homeland Security alert. These vulnerabilities, the most severe of which has a CVSS of 9.8 of 10 and all are rated critical, are tracked as follows:

1. CVE-2021-28480 – Microsoft Exchange Server Remote Code Execution Vulnerability
2. CVE-2021-28481 – Microsoft Exchange Server Remote Code Execution Vulnerability
3. CVE-2021-28482 – Microsoft Exchange Server Remote Code Execution Vulnerability
4. CVE-2021-28483 – Microsoft Exchange Server Remote Code Execution Vulnerability

Microsoft has provided a set of frequently asked questions regarding possible complications related to the installation of patches for these vulnerabilities. Microsoft also reported that the following four vulnerabilities were publicly exposed but not exploited:

1. CVE-2021-27091 – RPC Endpoint Mapper Service Elevation of Privilege Vulnerability
2. CVE-2021-28312 – Windows NTFS Denial of Service Vulnerability
3. CVE-2021-28437 – Windows Installer Information Disclosure Vulnerability – PolarBear
4. CVE-2021-28458 – Azure ms-rest-nodeauth Library Elevation of Privilege Vulnerability

Kaspersky researcher Boris Larin discovered a Win32k Elevation of Privilege Vulnerability (CVE-2021-28310) when it was being exploited in the wild, possibly by the BITTER APT group.

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 March, Adobe released security bulletins APSB21-20, APSB21-23, APSB21-26 and APSB21-28. These include patches for 10 vulnerabilities in its products, seven of which are categorized as critical. This includes Adobe Bridge, Adobe Digital Editions, Adobe Photoshop and RoboHelp, all rated as Priority 3. None of the CVEs addressed by Adobe were under active attack at the time of release. Users can update their software by using the auto-update feature of the product by selecting “Help” followed by, “Check for Updates” from their product menu. Alternatively, the latest version can be downloaded and installed manually. The full update installers can be downloaded from Adobe's Download Center.

INTEL

Intel did not release any vulnerability updates in April. Intel’s full archive of current and historic security updates can always be found here.

SAP

SAP released 19 security notes in April, five of them were updates to previous bugs. The most egregious of them affects version 6.5 of their Business Client platform, which received their highest severity score. This has a CVSS score of 10. There was also a remote code execution vulnerability in SAP Commerce which is tracked as CVE-2021-27602, affects SAP Commerce 1808, 1811, 1905, 2005, and 2011 and has a CVSS score of 9.8 out of 10. Another noteworthy bug categorized as critical is CVE-2021-21481, which is a missing authorization check vulnerability in versions 7.10, 7.11, 7.30, 7.31, 7.40 and 7.50 of the NetWeaver software stack. SAP scored the severity of this vulnerability at 9.6 out of 10 and the National Institute of Standards and Technology (NIST) scored it a base score of 8.8 (high-severity risk). The Department of Homeland Security also released an alert describing the active exploitation of relatively older vulnerabilities in a number of SAP products which have remained unpatched, based on joint research carried out by SAP and Onapsis. SAP advisories can always be found by logging into their support portal.

ORACLE

Oracle releases patches on a quarterly basis. In April, they released their most recent Critical Patch Update Advisory. This release contains 391 new security updates including patches for over 200 vulnerabilities that can be exploited remotely without authentication. Of these, 41 vulnerabilities are categorized as critical including five that feature a CVSS score of 10. Oracle’s E-Business Suite was the most patched of their products, receiving 70 fixes, of which 22 are remotely exploitable and do not require authentication. MySQL received patches for 49 vulnerabilities, 10 of which are remotely exploitable and do not require authentication. Fusion Middleware received patches for 45 vulnerabilities, with 36 exploitable without requiring authentication. Also, Retail Applications received 33 patches, with 31 exploitable without requiring authentication. Other platforms that were subject to high-priority fixes are Oracle Virtualization, ZFS Storage Appliance Kit, Cloud Infrastructure Storage Gateway and Storage Cloud Software Appliance.

The next four Oracle Critical Patch Update release dates are scheduled for:

- 20 July 2021
- 19 October 2021
- 18 January 2022
- 19 April 2022

CISCO

Cisco released 40 security advisories in April. Two of those - one related to their SD-WAN vManage Software and another related to their Small Business Routers – both of which are leveraged by the healthcare community and both were rated critical. These patches should be tested and deployed with the highest priority. There were also 10 rated “high”, including one related to Jabber and several related to their Firepower Threat Defense platform.

APPLE

Apple released security updates in April related to their iCloud, Xcode, Safari, macOS, iOS ad watchOS platforms. One of the more critical updates is for its macOS Big Sur operating system. This vulnerability, tracked as CVE-2021-30657, could allow an attacker to craft a payload in order to circumvent some of the security features by bypassing Gatekeeper, which enforces code signing and verifies downloaded applications.

DRUPAL

Drupal released a patch for a cross-site scripting vulnerability tracked as CVE-2020-13672 and categorized as critical.

References

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

Adobe Product Security Incident Response Team
https://helpx.adobe.com/security.html

Adobe Download & install help
https://helpx.adobe.com/download-install.html

Released: April 2021 Exchange Server Security Updates
https://techcommunity.microsoft.com/t5/exchange-team-blog/released-april-2021-exchange-server-security-updates/ba-p/2254617

NSA says it found new critical vulnerabilities in Microsoft Exchange Server
https://www.cyberscoop.com/nsa-microsoft-exchange-server-vulnerabilities/

Microsoft April 2021 Patch Tuesday fixes 108 flaws, 5 zero-days
https://www.bleepingcomputer.com/news/microsoft/microsoft-april-2021-patch-tuesday-fixes-108-flaws-5-zero-days/

Adobe Patches Slew of Critical Security Bugs in Bridge, Photoshop
https://threatpost.com/adobe-patches-critical-security-holes-bridge-photoshop/165371/

Adobe fixes critical vulnerabilities in Photoshop and Digital Editions
https://www.bleepingcomputer.com/news/security/adobe-fixes-critical-vulnerabilities-in-photoshop-and-digital-editions/

Adobe Releases Security Updates
https://us-cert.cisa.gov/ncas/current-activity/2021/04/13/adobe-releases-security-updates

SAP fixes critical bugs in Business Client, Commerce, and NetWeaver
https://www.bleepingcomputer.com/news/security/sap-fixes-critical-bugs-in-business-client-commerce-and-netweaver/

SAP Security Patch Day – April 2021
https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=573801649

Malicious Cyber Activity Targeting Critical SAP Applications
https://us-cert.cisa.gov/ncas/current-activity/2021/04/06/malicious-cyber-activity-targeting-critical-sap-applications

Attackers Actively Seeking, Exploiting Vulnerable SAP Applications
https://www.darkreading.com/threat-intelligence/attackers-actively-seeking-exploiting-vulnerable-sap-applications/d/d-id/1340602

SAP applications are getting compromised by skilled attackers https://www.helpnetsecurity.com/2021/04/07/sap-applications-compromised/

Active Cyberattacks on Mission-Critical SAP Applications
https://onapsis.com/active-cyberattacks-mission-critical-sap-applications

SAP and Onapsis Proactively Notify and Help Customers Protect Mission-Critical Applications from Active Cyber Threats
https://news.sap.com/2021/04/sap-onapsis-application-cyber-threat/

SAP issues advisory on the exploit of old vulnerabilities to target enterprise applications
https://www.zdnet.com/article/sap-issues-advisory-on-vulnerable-applications-being-widely-targeted-by-hackers/

Crooks are getting smarter about exploiting SAP software, study finds
https://www.cyberscoop.com/sap-cybercriminals-exploitation-onapsis/

Ongoing attacks are targeting unsecured mission-critical SAP apps
https://www.bleepingcomputer.com/news/security/ongoing-attacks-are-targeting-unsecured-mission-critical-sap-apps/

Oracle Critical Patch Update Advisory - April 2021
https://www.oracle.com/security-alerts/cpuapr2021.html

April 2021 Critical Patch Update: Executive Summary and Analysis
https://support.oracle.com/rs?type=doc&id=2765149.1

Oracle Critical Patch Update Advisory - April 2021
https://www.oracle.com/security-alerts/cpuapr2021.html

April 2021 Critical Patch Update: Executive Summary and Analysis
https://support.oracle.com/rs?type=doc&id=2765149.1

Microsoft Patch Tuesday, April 2021 Edition
https://krebsonsecurity.com/2021/04/microsoft-patch-tuesday-april-2021-edition/

Microsoft's April 2021 Patch Tuesday: Download covers 114 CVEs including new Exchange Server bugs
https://www.zdnet.com/article/microsoft-april-patch-download-covers-114-cves-including-new-exchange-server-bugs/

Microsoft’s April update patches 114 bugs—half of which allow remote code execution https://news.sophos.com/en-us/2021/04/13/microsofts-april-update-patches-114-bugs-more-than-half-of-which-allow-remote-code-execution/

Microsoft Patches 4 Additional Exchange Flaws
https://www.healthcareinfosecurity.com/microsoft-patches-4-additional-exchange-flaws-a-16396

Adobe Patches Slew of Critical Security Bugs in Bridge, Photoshop
https://threatpost.com/adobe-patches-critical-security-holes-bridge-photoshop/165371/

Microsoft Patch Tuesday for April 2021 — Snort rules and prominent vulnerabilities
https://blog.talosintelligence.com/2021/04/microsoft-patch-tuesday-for-april-2021.html

Microsoft April 2021 Patch Tuesday fixes 108 flaws, 5 zero-days
https://www.bleepingcomputer.com/news/microsoft/microsoft-april-2021-patch-tuesday-fixes-108-flaws-5-zero-days/

With court order, FBI removes hundreds of Exchange Server web shells from US organizations
https://www.cyberscoop.com/fbi-court-order-microsoft-exchange-server-web-shells/

Microsoft Patch Tuesday April 2021 fixes 108 vulnerabilities, including 5 zero-days
https://securityboulevard.com/2021/04/microsoft-patch-tuesday-april-2021-fixes-108-vulnerabilities-including-5-zero-days/

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback