CYBERSECURITY VULNERABILITIES OF INTEREST TO THE HEALTH SECTOR

In August, 2020, a significant number of vulnerabilities in common information systems relevant to the healthcare sector have been disclosed to the public. These vulnerabilities are from Microsoft, Adobe, Intel, Oracle, Cisco, SAP, 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

On Tuesday, August 11, Microsoft announced 120 vulnerabilities, the third largest number of Patch Tuesday fixes ever, including two actively exploited zero-days and a total of 17 critical and 103 important fixes. The first zero day is CVE-2020-1380, a scripting engine memory corruption vulnerability in Internet Explorer 11 which can allow for remote code execution. The second zero day is CVE-2020-1464, a spoofing vulnerability in the Windows file signature validation system. Both of these zero-day vulnerabilities were rated "critical" by Microsoft. Also worth noting is a vulnerability called "GlueBall", CVE-2020-1472, an elevation of privilege vulnerability that can be exploited if an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC). Below are 17 Patch Tuesday vulnerabilities rated Critical.

Vulnerable Technology	CVE	Brief Description
.NET Framework	CVE-2020-1046	.NET Framework Remote Code Execution Vulnerability
Internet Explorer	CVE-2020-1567	MSHTML Engine Remote Code Execution Vulnerability
Microsoft Edge	CVE-2020-1568	Microsoft Edge PDF Remote Code Execution Vulnerability
Microsoft Office	CVE-2020-1483	Microsoft Outlook Memory Corruption Vulnerability
Microsoft Scripting Engine	CVE-2020-1570	Scripting Engine Memory Corruption Vulnerability
Microsoft Scripting Engine	CVE-2020-1555	Scripting Engine Memory Corruption Vulnerability
Microsoft Video Control	CVE-2020-1492	Media Foundation Memory Corruption Vulnerability
Microsoft Windows Codecs Library	CVE-2020-1574	Microsoft Windows Codecs Library Remote Code Execution Vulnerability
Microsoft Windows Codecs Library	CVE-2020-1560	Microsoft Windows Codecs Library Remote Code Execution Vulnerability
Microsoft Windows Codecs Library	CVE-2020-1585	Microsoft Windows Codecs Library Remote Code Execution Vulnerability
Windows Media	CVE-2020-1379	Media Foundation Memory Corruption Vulnerability
Windows Media	CVE-2020-1554	Media Foundation Memory Corruption Vulnerability
Windows Media	CVE-2020-1339	Windows Media Remote Code Execution Vulnerability
Windows Media	CVE-2020-1525	Media Foundation Memory Corruption Vulnerability
Windows Media Player	CVE-2020-1477	Media Foundation Memory Corruption Vulnerability

Table 1: The fifteen critical Microsoft vulnerabilities (in addition to the two previously-described zero days) for August

In addition to the 17 critical vulnerabilities, the other Patch Tuesday vulnerabilities were rated as "important" by Microsoft. Cisco Talos released Snort rules to detect some of the exploitation attempts of the Microsoft Patch Tuesday vulnerabilities. Those rules can be found here.

On August 18, Microsoft announced that they would be discontinuing non-secure cipher suites supported by Microsoft Cloud App Security (MCAS), which is Microsoft's multimode cloud-based security solution that integrates with other platforms such as Azure Active Directory, Azure Security Center, and Microsoft Defender ATP to detect and prevent cyberthreats across Microsoft and third-party cloud services.

On August 19, Microsoft released an out-of-band security update to address privilege escalation bugs found to impact the Windows Remote Access service for Windows 8.1 and Windows Server 2012 R2. The two vulnerabilities are CVE-2020-1530 and CVE-2020-1537. The first addresses an elevation of privilege vulnerability when Windows Remote Access improperly handles memory. The second addresses elevation of privilege vulnerability when Windows Remote Access improperly handles file operations.

ADOBE

Adobe released August Patch Tuesday security updates (APSB20-48) for its Acrobat, Reader and Lightstream products. They released fixes for 25 vulnerabilities. Eleven of these are rated critical and if exploited, allow for the arbitrary execution of code.

Vulnerability Category	Impact	CVE
Out-of-bounds write	Arbitrary Code Execution	CVE-2020-9693
Out-of-bounds write	Arbitrary Code Execution	CVE-2020-9694
Security bypass	Security feature bypass	CVE-2020-9696
Security bypass	Security feature bypass	CVE-2020-9712
Buffer error	Arbitrary Code Execution	CVE-2020-9698
Buffer error	Arbitrary Code Execution	CVE-2020-9699
Buffer error	Arbitrary Code Execution	CVE-2020-9700
Buffer error	Arbitrary Code Execution	CVE-2020-9701
Buffer error	Arbitrary Code Execution	CVE-2020-9704
Use-after-free	Arbitrary Code Execution	CVE-2020-9715
Use-after-free	Arbitrary Code Execution	CVE-2020-9722

INTEL

Intel released 18 security advisories covering 52 vulnerabilities for their August 2020 Patch Tuesday release. The highlights are as follows:

Intel wireless Bluetooth products that may allow denial of service, information disclosure or escalation of privilege if exploited. These affect Intel Wireless Bluetooth products on Windows, Chrome OS and Linux OS.

- Intel released firmware and software updates to mitigate these potential vulnerabilities. These include the following CVE:
  - CVE-2020-0554
    - CVSS Score: 8.6
  - CVE-2020-0555
    - CVSS Score: 8.4
  - CVE-2020-0553
    - CVSS Score: 4.4
  - CVE-2019-14620
    - CVSS Score: 4.3
- Intel released firmware updates to mitigate escalation of privilege vulnerabilities in several Intel server board families. These include the following:
  - CVE-2020-12300
    - CVSS Score: 7.5
  - CVE-2020-12301
    - CVSS Score: 7.5
  - CVE-2020-12299
    - CVSS Score: 6.7

- Intel released firmware updates to mitigate vulnerabilities in some of their server boards, server systems and compute modules may allow escalation of privilege or denial of service. These include the following CVEs:
    - CVE-2020-8708
        - CVSS 9.6
    - CVE-2020-8730
        - CVSS Score: 8.8
    - CVE-2020-8731
        - CVSS Score: 8.8
    - CVE-2020-8707
        - CVSS Score: 8.3
    - CVE-2020-8719
        - CVSS Score: 8.2
    - CVE-2020-8721
        - CVSS Score: 8.2
    - CVE-2020-8710
        - CVSS Score: 8.2
    - CVE-2020-8711
        - CVSS Score: 8.2
    - CVE-2020-8712
        - CVSS Score: 8.2
    - CVE-2020-8718
        - CVSS Score: 7.8
    - CVE-2020-8722
        - CVSS Score: 7.5
    - CVE-2020-8732
        - CVSS Score: 6.3
    - CVE-2020-8709
        - CVSS Score: 6.1
    - CVE-2020-8723
        - CVSS Score: 5.4
    - CVE-2020-8713
        - CVSS Score: 4.7
    - CVE-2020-8706
        - CVSS Score: 4.7
    - CVE-2020-8729
        - CVSS Score: 4.4
    - CVE-2020-8715
        - CVSS Score: 4.3
    - CVE-2020-8716
        - CVSS Score: 3.8
    - CVE-2020-8714
        - CVSS Score: 3.8
    - CVE-2020-8717
        - CVSS Score: 3.3
    - CVE-2020-8720
        - CVSS Score: 2.3

ORACLE

Oracle releases patches on a quarterly basis. Their most recent release was their 2020 Q2 bulletin which weas released in July and can be found here.

CISCO

Cisco recently released several vulnerability patches. All their advisories can be found in their repository. There are two of these which are the highest priority. There are vulnerabilities the Treck IP stack implementation (commonly known as Ripple 20) associated with CVE-2020-3466 with the patch information available here. This vulnerability has ben rated critical with a CVSS score of 9.8. The second set of vulnerabilities are in Cisco's Virtual Wide Area Application Services (vWAAS). These are associated with CVE-2020-3446, have a CVSS score of 9.8 and if exploited, allow for remote, unauthenticated access to the device interface.

SAP

SAP released 15 security advisories on Patch Tuesday this month and two of them are critical. These are advisory #2934135 which involves a lack of authentication check vulnerability (CVE-2020-6287) with a CVSS score of 10.0 and advisory #2928635insufficient input path validation (Cross-site scripting) vulnerability (CVE-2020-6286) with a CVSS score of 9, both in their in their Netweaver platform. Further details can be found here or by logging into their support portal.

APPLE

Apple released updates for iCloud for Windows. These are particularly important for healthcare organizations who have a bring-your-own-device (BYOD) policy or that include apple mobile devices as part of their enterprise infrastructure. One set of vulnerabilities is associated with iCloud for Windows 7.20 and the second set of vulnerabilities is associated with iCloud for Windows 11.3.

GOOGLE

Google released Chrome version 85 this month and it includes new security features and APIs. It protects the system from mixed-content downloads and provides security for same-site cookies. It also includes new features such as 10% faster page loads and a QR generator.

REFERENCES

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

Microsoft August 2020 Patch Tuesday fixes 2 zero-days, 120 flaws
https://www.bleepingcomputer.com/news/microsoft/microsoft-august-2020-patch-tuesday-fixes-2-zero-days-120-flaws/

CISA Bulletin (SB20-237) Vulnerability Summary for the Week of August 17, 2020
https://us-cert.cisa.gov/ncas/bulletins/sb20-237

Microsoft's August 2020 Patch Tuesday Addresses 120 CVEs (CVE-2020-1337)
https://www.tenable.com/blog/microsoft-s-august-2020-patch-tuesday-addresses-120-cves-cve-2020-1337

August 2020 Patch Tuesday: Microsoft fixes two vulnerabilities under attack
https://www.helpnetsecurity.com/2020/08/11/august-2020-patch-tuesday/

Security update for Windows 8.1, RT 8.1, and Server 2012 R2: August 19, 2020
https://support.microsoft.com/en-us/help/4578013/security-update-for-windows-8-1-rt-8-1-and-server-2012-r2

CVE-2020-1530 | Windows Remote Access Elevation of Privilege Vulnerability
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1530

CVE-2020-1537 | Windows Remote Access Elevation of Privilege Vulnerability
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1537

End of support for non-secure cipher suites in Microsoft Cloud App Security
https://techcommunity.microsoft.com/t5/microsoft-security-and/end-of-support-for-non-secure-cipher-suites-in-microsoft-cloud/ba-p/1596262

Oracle Critical Patch Update Advisory - July 2020
https://www.oracle.com/security-alerts/cpujul2020.html

"GlueBall" Microsoft Windows Spoofing Vulnerability – Expert Source
https://www.informationsecuritybuzz.com/expert-comments/glueball-microsoft-windows-spoofing-vulnerability-expert-source/

Microsoft apparently just fixed a Windows security flaw first reported to it in 2018
https://www.neowin.net/news/microsoft-apparently-just-fixed-a-windows-security-flaw-first-reported-to-it-in-2018

Researchers Find More Devices, Vendors Vulnerable to Ripple20
https://healthitsecurity.com/news/researchers-find-more-devices-vendors-vulnerable-to-ripple20

Multiple Vulnerabilities in Treck IP Stack Affecting Cisco Products: June 2020
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-treck-ip-stack-JyBQ5GyC

Cisco vWAAS for Cisco ENCS 5400-W Series and CSP 5000-W Series Default Credentials Vulnerability
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-waas-encsw-cspw-cred-hZzL29A7

Talos Rules 2020-08-11
https://snort.org/advisories/talos-rules-2020-08-11