LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

HC3: Monthly Cybersecurity Vulnerability Bulletin

June 11, 2021 TLP: White Report: 202106111200

News of Interest to the Health Sector

- MITRE updated to version 9 their ATT&CK framework for analyzing and characterizing cyber threats.
- Emsisoft recently released a report titled: *The Cost of Ransomware in 2021 – a Country-by-country Analysis*. For the year 2020, their data shows the average ransom demand grew by more than 80%. For aggregate ransom costs, the data sample they have access to shows that a minimum of $18.6 billion was paid globally last year, however, it is estimated the real total is around $75B globally. Reports all state US victims paid a minimum ~$1B, but estimate the total may be as much as $3.7B. That cost increases significantly when factoring in downtime costs, and this may provide a little more insight as to why organizations pay ransom. Including downtime costs, US victims paid a minimum of about $5B and are estimated to have paid as much as $20B
- Sophos released their *State of Ransomware in Healthcare 2021* report. They surveyed decision makers in healthcare organizations across 30 countries and found one third (about 34%) of all healthcare organizations were successfully attacked by ransomware over the last year. It was also found that healthcare was a bit less able to prevent ransomware attacks. 54% of all ransomware attacks resulted in encrypted data across industries, that number was 65% when limited to healthcare organizations. They also found healthcare organizations were a bit more likely to pay ransom – 34% of healthcare organizations attacked by ransomware paid up, while the average across industries was 32%. However, healthcare organizations were less likely to use backups to restore data, only 44% reported doing so as compared to the 57% average across industries. The average cost of a ransom for healthcare organizations according to their data was lower as compared to other industries – about $130K for healthcare and about $170K for all survey respondents. Finally, average ransomware recovery costs were much lower for healthcare as compare to other industries: Healthcare averaged $1.2 million in recovery costs while the rest of the industry averaged $1.85 million, with education coming in first at $2.73 million on average. Sophos provided two possible reasons for this: First, many healthcare organizations don't have the IT budgets that other sectors do. Also, in many parts of the world, healthcare is a public service and therefore there are less reputational costs. In a competitive market, if people lose faith in one health provider, they can choose to use another. When healthcare is strictly a public service, they tend to be less concerned with their brand and losing patients to competitors.
- The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency released a best practices guide specifically for Darkside ransomware. HC3 recommends this guide for many reasons. First, as ransomware operators, Darkside remains a general threat to healthcare, regardless of their targeting history. Second, this guide presents not just strong advice for Darkside, but much of it applies across ransomware families and even represents good general cyber hygiene practices. Third, this guide contains several references which will be helpful for the healthcare organization attempting to remain as secure as possible in cyberspace.

Vulnerabilities of Interest to the Health Sector

Executive Summary

In May 2021, vulnerabilities in common information systems relevant to the healthcare sector have been disclosed to the public and 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 April 2021 Patch Tuesday, Microsoft released 55 patches, which included three zero-days, four classified as "critical" (with three of those four remote code execution), none of them known to be actively exploited in the wild. The most important of the zero days is CVE-2021-31207, which is a security bypass vulnerability in Exchange Server. The other two zero-days are CVE-2021-31204, a .NET and Visual Studio Elevation of Privilege vulnerability, and CVE-2021-31200, a Common Utilities Remote Code Execution vulnerability. Of the four categorized as critical, CVE-2021-31166, an HTTP protocol stack remote code execution vulnerability in Windows, is the most noteworthy. If an unauthenticated attacker sends a specially crafted packet to a vulnerable system, it allows them to execute code as kernel – at the operating system level. This makes the vulnerability potentially wormable (self-propagating) and as such, CVE-2021-31166 should also be treated as a priority. See Appendix A, located below, for the full list of Microsoft vulnerabilities for the month of May.

ADOBE

In May, Adobe released security bulletin APSB21-29, which patches 44 vulnerabilities across 12 different products. The most important one in this group is CVE-2021-28550, a remote code execution vulnerability in Acrobat and Reader which has been exploited in the wild. This is one of many vulnerabilities in Adobe Acrobat and Reader for Windows and macOS that should be prioritized for patching because they fix several critical and important vulnerabilities in a common product that is frequently targeted. The Experience Manager should be prioritized next as it has also been historically targeted, although not as much as Acrobat or Reader. The patch fixes multiple vulnerabilities, one of which – CVE-2021-21084 – could allow attackers to execute arbitrary JavaScript in the user's browser. The full update installers can always be downloaded from Adobe's Download Center.

INTEL

Intel released one security advisory in May, related to several of their wireless (WiFi) products. This patch addresses three vulnerabilities:

- CVE-2020-24586 – An unpatched device does not clear its cache/memory from previous session after reconnection/reassociation which can allow for a fragment cache attack.
- CVE-2020-24587 – An unpatched device reassembles fragments encrypted under different keys in a protected network allowing for a possible mixed key attack.
- CVE-2020-24588 - An unpatched device can allow the encrypted payload to be parsed as containing one or more aggregated frames instead of a normal network packet, allowing for a possible frame aggregation attack.

Intel's full archive of current and historic security updates can be found here.

SAP

SAP released 14 new and updated security patches in May. The most important are:

- An update to a security note released in 2018 for the browser control Google Chromium delivered with SAP Business Client (CVSS: 10)
- An update to security note released in April 2021 (CVE-2021-27602) which is a remote code execution vulnerability in the source rules of SAP Commerce (CVSS: 9.9)
- An update to security note released in January 2021 (CVE-2021-21466) which is a code injection in SAP Business Warehouse and SAP BW/4HANA (CVSS: 9.9)
- A code injection vulnerability (CVE-2021-27611) in SAP NetWeaver AS ABAP (CVSS: 8.2)

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

ORACLE

Oracle releases patches on a quarterly basis. In April, they released their 2021 Q1 Critical Patch Update Advisory included 391 patches across many of their products and third-party components as part of their products. The next release is expected in July 2021.

CISCO

Cisco released 45 security advisories in May, two of them categorized as critical potentially enabling remote execution as root or the creation of rogue admin accounts. The first critical advisory, command injection vulnerabilities in the HyperFlex HX platform, are tracked as CVE-2021-1497 and CVE-2021-1498. These could allow an unauthenticated, remote attacker to perform command injection attacks against an affected device. The second critical advisory, multiple vulnerabilities in the SD-WAN vManage software platform could allow an unauthenticated, remote attacker to execute arbitrary code or gain access to sensitive information, escalate privileges or gain unauthorized access to the application. These are associated with CVE-2021-1275, CVE-2021-

1468, CVE-2021-1505, CVE-2021-1506 and CVE-2021-1508. Cisco also released 12 security alerts classified as high, which should be prioritized for applicability and patching. Cisco did not report any active exploitation of these vulnerabilities at the time of publishing.

APPLE

Apple released security updates in May for Safari, Catalina, Mjoave, iOS.iPadOS, Boot Camp and watchOS. Several of these were actively exploited Webkit vulnerabilities.

Appendix A – Full list of Microsoft Vulnerabilities (Source: Zero Day Initiative)

CVE	Title	Severity	CVSS	Public	Exploited	Type
CVE-2021-31204	.NET Core and Visual Studio Elevation of Privilege Vulnerability	Important	7.3	Yes	No	EoP
CVE-2021-31200	Common Utilities Remote Code Execution Vulnerability	Important	7.2	Yes	No	RCE
CVE-2021-31207	Microsoft Exchange Server Security Feature Bypass Vulnerability	Moderate	6.6	Yes	No	SFB
CVE-2021-31166	HTTP Protocol Stack Remote Code Execution Vulnerability	Critical	9.8	No	No	RCE
CVE-2021-28476	Hyper-V Remote Code Execution Vulnerability	Critical	9.9	No	No	RCE
CVE-2021-31194	OLE Automation Remote Code Execution Vulnerability	Critical	7.8	No	No	RCE
CVE-2021-26419	Scripting Engine Memory Corruption Vulnerability	Critical	6.4	No	No	RCE
CVE-2021-28461	Dynamics Finance and Operations Cross-site Scripting Vulnerability	Important	6.1	No	No	XSS
CVE-2021-31936	Microsoft Accessibility Insights for Web Information Disclosure Vulnerability	Important	7.4	No	No	Info
CVE-2021-31182	Microsoft Bluetooth Driver Spoofing Vulnerability	Important	7.1	No	No	Spoofing
CVE-2021-31174	Microsoft Excel Information Disclosure Vulnerability	Important	5.5	No	No	Info
CVE-2021-31195	Microsoft Exchange Server Remote Code Execution Vulnerability	Important	6.5	No	No	RCE

CVE	Title	Severity	CVSS	Public	Exploited	Type
CVE-2021-31198	Microsoft Exchange Server Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2021-31209	Microsoft Exchange Server Spoofing Vulnerability	Important	6.5	No	No	Spoofing
CVE-2021-28455	Microsoft Jet Red Database Engine and Access Connectivity Engine Remote Code Execution Vulnerability	Important	8.8	No	No	RCE
CVE-2021-31180	Microsoft Office Graphics Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2021-31178	Microsoft Office Information Disclosure Vulnerability	Important	5.5	No	No	Info
CVE-2021-31175	Microsoft Office Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2021-31176	Microsoft Office Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2021-31177	Microsoft Office Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2021-31179	Microsoft Office Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2021-31171	Microsoft SharePoint Information Disclosure Vulnerability	Important	4.1	No	No	Info
CVE-2021-31181	Microsoft SharePoint Remote Code Execution Vulnerability	Important	8.8	No	No	RCE
CVE-2021-31173	Microsoft SharePoint Server Information Disclosure Vulnerability	Important	5.3	No	No	Info
CVE-2021-28474	Microsoft SharePoint Server Remote Code Execution Vulnerability	Important	8.8	No	No	RCE
CVE-2021-26418	Microsoft SharePoint Spoofing Vulnerability	Important	4.6	No	No	Spoofing
CVE-2021-28478	Microsoft SharePoint Spoofing Vulnerability	Important	7.6	No	No	Spoofing

CVE	Title	Severity	CVSS	Public	Exploited	Type
CVE-2021-31172	Microsoft SharePoint Spoofing Vulnerability	Important	7.1	No	No	Spoofing
CVE-2021-31184	Microsoft Windows Infrared Data Association (IrDA) Information Disclosure Vulnerability	Important	5.5	No	No	Info
CVE-2021-26422	Skype for Business and Lync Remote Code Execution Vulnerability	Important	7.2	No	No	RCE
CVE-2021-26421	Skype for Business and Lync Spoofing Vulnerability	Important	6.5	No	No	Spoofing
CVE-2021-31214	Visual Studio Code Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2021-31211	Visual Studio Code Remote Development Extension Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2021-31213	Visual Studio Code Remote Development Extension Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2021-27068	Visual Studio Remote Code Execution Vulnerability	Important	8.8	No	No	RCE
CVE-2021-28465	Web Media Extensions Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2021-31190	Windows Container Isolation FS Filter Driver Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-31165	Windows Container Manager Service Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-31167	Windows Container Manager Service Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-31168	Windows Container Manager Service Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP

CVE	Title	Severity	CVSS	Public	Exploited	Type
CVE-2021-31169	Windows Container Manager Service Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-31208	Windows Container Manager Service Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-28479	Windows CSC Service Information Disclosure Vulnerability	Important	5.5	No	No	Info
CVE-2021-31185	Windows Desktop Bridge Denial of Service Vulnerability	Important	5.5	No	No	DoS
CVE-2021-31170	Windows Graphics Component Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-31188	Windows Graphics Component Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-31192	Windows Media Foundation Core Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2021-31191	Windows Projected File System FS Filter Driver Information Disclosure Vulnerability	Important	5.5	No	No	Info
CVE-2021-31186	Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability	Important	7.4	No	No	Info
CVE-2021-31205	Windows SMB Client Security Feature Bypass Vulnerability	Important	4.3	No	No	SFB
CVE-2021-31193	Windows SSDP Service Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-31187	Windows WalletService Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2020-24587	Windows Wireless Networking Information Disclosure Vulnerability	Important	6.5	No	No	Info

CVE	Title	Severity	CVSS	Public	Exploited	Type
CVE-2020-24588	Windows Wireless Networking Spoofing Vulnerability	Important	6.5	No	No	Spoofing
CVE-2020-26144	Windows Wireless Networking Spoofing Vulnerability	Important	6.5	No	No	Spoofing

References

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

- Apple Releases Security Updates
  https://us-cert.cisa.gov/ncas/current-activity/2021/05/04/apple-releases-security-updates

- Cisco bugs allow creating admin accounts, executing commands as root
  https://www.bleepingcomputer.com/news/security/cisco-bugs-allow-creating-admin-accounts-executing-commands-as-root/

- Google's Android operating system update for May 2021 addresses a total of 42 vulnerabilities, four of which are marked as critical severity.
  https://news.softpedia.com/news/android-releases-updates-for-may-2021-which-patches-over-40-vulnerabilities-532811.shtml

- Cisco Releases Security Updates for Multiple Products
  https://us-cert.cisa.gov/ncas/current-activity/2021/05/06/cisco-releases-security-updates-multiple-products

- Cisco fixes 6-month-old AnyConnect VPN zero-day with exploit code
  https://www.bleepingcomputer.com/news/security/cisco-fixes-6-month-old-anyconnect-vpn-zero-day-with-exploit-code/

- May Android security updates patch 4 zero-days exploited in the wild
  https://www.bleepingcomputer.com/news/security/may-android-security-updates-patch-4-zero-days-exploited-in-the-wild/

- Cisco Releases Security Updates for Multiple Products
  https://us-cert.cisa.gov/ncas/current-activity/2021/05/19/cisco-releases-security-updates-

multiple-products

- May 2021 Patch Tuesday: Adobe fixes exploited Reader 0-day, Microsoft patches 55 holes
https://www.helpnetsecurity.com/2021/05/12/may-2021-patch-tuesday/

- Microsoft's May 2021 Patch Tuesday: 55 flaws fixed, four critical
https://www.zdnet.com/article/microsofts-may-2021-patch-tuesday-55-flaws-fixed-four-critical/

- The May 2021 Security Update Review
https://www.zerodayinitiative.com/blog/2021/5/11/the-may-2021-security-update-review

- Microsoft Patch Tuesday, May 2021 Edition
https://krebsonsecurity.com/2021/05/microsoft-patch-tuesday-may-2021-edition/

- Microsoft Fixes Exchange Server Zero-Day in May Patch Tuesday
https://www.infosecurity-magazine.com/news/microsoft-exchange-server-zeroday/

- Adobe fixes Reader zero-day vulnerability exploited in the wild
https://www.bleepingcomputer.com/news/security/adobe-fixes-reader-zero-day-vulnerability-exploited-in-the-wild/

- Microsoft May 2021 Patch Tuesday fixes 55 flaws, 3 zero-days
https://www.bleepingcomputer.com/news/microsoft/microsoft-may-2021-patch-tuesday-fixes-55-flaws-3-zero-days/

- Wormable Windows Bug Opens Door to DoS, RCE
https://threatpost.com/wormable-windows-bug-dos-rce/166057/

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