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

HC3: Monthly Cybersecurity Vulnerability Bulletin

August 18, 2021 TLP: White Report: 202108180830

News of Interest to the Health Sector

- The Kaseya cyberattack was one of the biggest managed service provider cyberattacks in history. On Friday, July 2, the software company Kaseya became aware of a compromise of their Virtual System Administrator (VSA) platform, which is remote monitoring and endpoint management software they sell to their customer base of managed service providers. Immediately after the attack, they shut down VSA in accordance with their playbook, within an hour and the Department of Homeland Security and Federal Bureau of Investigation became involved immediately. They estimated that between 50 and 60 of their customers were impacted and those impacted customers – managed service providers – are believed to manage IT services for about 1,500 companies and organizations. The ransomware operators, REvil (AKA Sodinokibi) claimed responsibility. Initially, REvil offered a universal decryptor for $70 million in Bitcoin and reports noted that the demand dropped to $50 million shortly thereafter. Kaseya was in the process of testing and validating the patch. They were previously notified of the vulnerability by the Dutch Institute for Vulnerability Disclosure. It's been given the identifier CVE-2021-30116. CISA and FBI jointly released guidance and a free Kaseya VSA compromise detection tool which looks for indicators of compromise. The White house stated that they did not believe the Russian government was the source of these attacks but instead criminal groups physically located in Russia. Kaseya announced that they obtained a decryptor key (no further details on how) and are working with customers to restore operations. Because details of compromises are often kept private, it is not known if (or how many) healthcare or public health organizations were impacted by the Kaseya cyberattack. REvil has not been operational since the Kaseya attack and speculation is they disbanded and rebranded or disbursed to other cybercriminal groups.
- The company BitDefender shared some recent research exclusively with the Department of Defense. This research implies that the TrickBot are becoming fully operational once again, despite having both US Cyber Command and Microsoft carry out sustained disruptive attacks against them last October. In June, the Department of Justice indicted and charged a Latvian-national named Alla Witte, for conspiracy to commit computer fraud and aggravated identify theft as part of her work with TrickBot. Back in February, Menlo Security reported observing an Emotet campaign that was dropping Trickbot – That combination has historically been common, especially in facilitating ransomwares attacks against healthcare targets. This BitDefender research has not been made public yet, but it likely reveals significant activity if they thought enough of it to share it with the DoD. Historically, the TrickBot operators have targeted the healthcare industry heavily.
- Fortified Security released a report titled, 2021 mid-year review: The State of Cybersecurity in Healthcare. When compared to their data from a year ago, they found a 185% increase in the number of patients impacted by healthcare breaches. Last summer, there had been just under 8 million patients impacted by healthcare breaches for the first half of the year. This year, there have been just under 23 million patients impacted by healthcare data breaches. For the breaches in 2021, 73% of the them were due to compromise of healthcare provider. Another 16% were due to compromise of health plans and 11% were due to compromise of business associates. In terms of technical causes, cyberattacks were responsible for 73% of all breaches. Unauthorized access or other accidental disclosure accounted for another 22%, and the remaining 5% were caused by smaller thefts, lost hardware, or improper disposals.
- In late July, IBM released their annual Cost of a Data Breach report. In it, they assessed data breaches in 2021 cost a company $4.24 million on average per incident, which is the highest figure in the 17-year history of the report. In the United States, a data breach cost about $9 million on average per incident. The cost of breaches increased about 10% in a year, and IBM largely attributes som of that to the remote workforce which has increasingly been in place since the beginning of the pandemic. IBM also found that the average cost of a breach increased about $1 million when remote work was a factor in the breach. It's worth noting that breaches in the healthcare industry were more expensive than any other industry, and that was the 11th year in a row that that was the case. The average healthcare breach was $9.23 million, which was a dramatic increase, about 30%, from the $7.13 million it was in 2019.

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

HC3: Monthly Cybersecurity Vulnerability Bulletin

August 18, 2021 TLP: White Report: 202108180830

Vulnerabilities of Interest to the Health Sector from the Month of July

Executive Summary

In July 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, 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. As always, an effective patch management program begins with proper inventory management and asset tracking.

Report

MICROSOFT

In July 2021, Microsoft patched 117 vulnerabilities, a significant increase from recent Patch Tuesday releases. In terms of severity, there were 9 zero-days, 13 were classified as critical, 1 moderate, and 103 as important. In terms of types of vulnerabilities, the most noteworthy data point is that 44 are remote code execution, with 32 are escalation of privilege, 14 information disclosure, 12 Denial of Service, 8 security bypass, and 7 spoofing vulnerabilities. Of those nine zero days, five were publicly disclosed, but not known to be exploited. However, there are three zero days that have been actively exploited:

- CVE-2021-33771 – Windows Kernel Elevation of Privilege Vulnerability
- CVE-2021-34448 – Scripting Engine Memory Corruption Vulnerability
- CVE-2021-31979 - Windows Kernel Elevation of Privilege Vulnerability

Microsoft also had several security issues starting in June and into July associated with their print spooler technology – the software component of their desktop and server operating systems which manages print drivers as well as individual print jobs, including receiving files to be printed, queueing, scheduling and initiating printing. The label PrintNightmare has been used for some of these vulnerabilities and has caused some confusion and misinformation to be spread. Furthermore, one of the patches that Microsoft released only patched part of the vulnerability in question and additional mitigation steps are needed in order to improve security. In an effort to be clear and accurate, below is a summary of those vulnerabilities:

- Microsoft released a patch for a remote code execution and privilege escalation vulnerability in their Print Spooler, tracked as CVE-2021-1675.
- A second remote code execution and privilege escalation vulnerability in Windows Print Spooler (distinct from CVE-2020-1575) was public ally-released as a zero day and eventually patched by

Microsoft. It is tracked as CVE-2021-34527.

- As it turned out, CVE-2021-34527 didn't fix the escalation of privilege but only the remote code execution part of the vulnerability. Additional mitigations and registry modifications are recommended, with details being found on Microsoft's website.
- Another Escalation of Privilege vulnerability was found in the Windows Print Spooler. This is being tracked as CVE-2021-34481. Additional mitigations and registry modifications are recommended, with details being found on Microsoft's website.
- For all Print Spooler vulnerabilities including the ones listed in this bulletin, it is recommended as the best possible action to reduce an organization's attack surface to disable Print Spooler services on individual systems entirely whenever possible. This can only be done or systems that don't need to print, but it's the only way of being absolutely sure that Print Spool vulnerabilities cannot impact infrastructure.

ADOBE

Adobe released 5 patches on Patch Tuesday and an additional 7 patches later in the month. This includes critical fixes in Acrobat, Reader, Dimension and Bridge. The archive of Adobe Security Bulletins and Advisories can be found here.

INTEL

Intel did not release any patches in the month of July. This was following the release of 73 patches in June, which was the first time in several months they released a large group together. Intel patches can be found on the official Intel Product Security Center Advisory page.

SAP

SAP released 12 security notes in July. Four of these are recommended to be considered to be possibly high priority by healthcare organizations, depending on what software they have deployed:

- Update to Security Note regarding security updates for the browser control Google Chromium delivered with SAP Business Client (Note: 2622660, CVSS: 10)
- Update to Security Note released on June 2021 Patch Tuesday – Improper Authentication in SAP NetWeaver ABAP Server and ABAP Platform (Note: 3007182, CVSS: 9, CVE-2021-27610)
- Missing Authorization check in SAP NetWeaver Guided Procedures (Note: 3059446, CVSS: 7.6, CVE-2021-33671)
- Denial of Service (DoS) in SAP NetWeaver AS for Java (Note: 3056652, CVSS: 7.5, CVE-2021-33670)

More information on SAP vulnerabilities can be found on their Security Response at SAP Home page.

CISCO

Cisco released 25 security advisories in July. None of those were rated critical and 8 were rated high. Of those, the most important were:

- IOS and IOS XE Software Bidirectional Forwarding Detection Denial of Service Vulnerability
- Intelligent Proximity SSL Certificate Validation Vulnerability
- FXOS and NX-OS Software Simple Network Management Protocol Denial of Service Vulnerability
- Business Process Automation Privilege Escalation Vulnerabilities
- Update - Multiple Vulnerabilities in OpenSSL Affecting Cisco Products: March 2021
- Web Security Appliance Privilege Escalation Vulnerability

APPLE

Apple released a patch for an iOS and macOS zero-day vulnerability, tracked as CVE-2021-30807, which is a zero day that impacts iOS, iPadOS, and macOS. This was the 13th zero day patch from Apple to date this year.

APACHE

Apache released a security advisory for various versions of the Tomcat web platform, tracked as CVE-2021-33037, which when compromised can allow for information leakage.

VMWARE

VMware released patches for vulnerabilities in VMware ESXi and VMware Cloud Foundation. These are detailed in their advisory, VMSA-2021-0014, and are tracked CVE-2021-21994 and CVE-2021-21995 which cover improper authentication and denial of service issues.

CITRIX

Citrix released security update CTX319750 which covers a vulnerability in for their Virtual Apps and Desktops which could allow for privilege escalation.

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

CVE	Title	Severity	CVSS	Public	Exploited	Type
CVE-2021-34527	Windows Print Spooler Remote Code Execution Vulnerability	Critical	8.8	Yes	Yes	RCE
CVE-2021-34448	Scripting Engine Memory Corruption Vulnerability	Critical	6.8	No	Yes	RCE
CVE-2021-31979	Windows Kernel Elevation of Privilege Vulnerability	Important	7.8	No	Yes	EoP
CVE-2021-33771	Windows Kernel Elevation of Privilege Vulnerability	Important	7.8	No	Yes	EoP
CVE-2021-34473	Microsoft Exchange Server Remote Code Execution Vulnerability	Critical	9.1	Yes	No	RCE

CVE	Title	Severity	CVSS	Public	Exploited	Type
CVE-2021-33781	Active Directory Security Feature Bypass Vulnerability	Important	8.1	Yes	No	SFB
CVE-2021-34523	Microsoft Exchange Server Elevation of Privilege Vulnerability	Important	9	Yes	No	EoP
CVE-2021-33779	Windows ADFS Security Feature Bypass Vulnerability	Important	8.1	Yes	No	SFB
CVE-2021-34492	Windows Certificate Spoofing Vulnerability	Important	8.1	Yes	No	Spoofing
CVE-2021-34474	Dynamics Business Central Remote Code Execution Vulnerability	Critical	8	No	No	RCE
CVE-2021-34464	Microsoft Defender Remote Code Execution Vulnerability	Critical	7.8	No	No	RCE
CVE-2021-34522	Microsoft Defender Remote Code Execution Vulnerability	Critical	7.8	No	No	RCE
CVE-2021-34439	Microsoft Windows Media Foundation Remote Code Execution Vulnerability	Critical	7.8	No	No	RCE
CVE-2021-34503	Microsoft Windows Media Foundation Remote Code Execution Vulnerability	Critical	7.8	No	No	RCE
CVE-2021-34494	Windows DNS Server Remote Code Execution Vulnerability	Critical	8.8	No	No	RCE
CVE-2021-34450	Windows Hyper-V Remote Code Execution Vulnerability	Critical	8.5	No	No	RCE
CVE-2021-34458	Windows Kernel Remote Code Execution Vulnerability	Critical	9.9	No	No	RCE
CVE-2021-33740	Windows Media Remote Code Execution Vulnerability	Critical	7.8	No	No	RCE

CVE	Title	Severity	CVSS	Public	Exploited	Type
CVE-2021-34497	Windows MSHTML Platform Remote Code Execution Vulnerability	Critical	6.8	No	No	RCE
CVE-2021-34476	Bowser.sys Denial of Service Vulnerability	Important	7.5	No	No	DoS
CVE-2021-34489	DirectWrite Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2021-34440	GDI+ Information Disclosure Vulnerability	Important	5.5	No	No	Info
CVE-2021-31947	HEVC Video Extensions Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2021-33775	HEVC Video Extensions Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2021-33776	HEVC Video Extensions Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2021-33777	HEVC Video Extensions Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2021-33778	HEVC Video Extensions Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2021-33760	Media Foundation Information Disclosure Vulnerability	Important	5.5	No	No	Info
CVE-2021-33753	Microsoft Bing Search Spoofing Vulnerability	Important	4.7	No	No	Spoofing
CVE-2021-34501	Microsoft Excel Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2021-34518	Microsoft Excel Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2021-33766	Microsoft Exchange Information Disclosure Vulnerability	Important	7.3	No	No	Info

CVE	Title	Severity	CVSS	Public	Exploited	Type
CVE-2021-33768	Microsoft Exchange Server Elevation of Privilege Vulnerability	Important	8	No	No	EoP
CVE-2021-34470	Microsoft Exchange Server Elevation of Privilege Vulnerability	Important	8	No	No	EoP
CVE-2021-31196	Microsoft Exchange Server Remote Code Execution Vulnerability	Important	7.2	No	No	RCE
CVE-2021-31206	Microsoft Exchange Server Remote Code Execution Vulnerability	Important	7.6	No	No	RCE
CVE-2021-34451	Microsoft Office Online Server Spoofing Vulnerability	Important	5.3	No	No	Spoofing
CVE-2021-34469	Microsoft Office Security Feature Bypass Vulnerability	Important	8.2	No	No	SFB
CVE-2021-34467	Microsoft SharePoint Server Remote Code Execution Vulnerability	Important	7.1	No	No	RCE
CVE-2021-34468	Microsoft SharePoint Server Remote Code Execution Vulnerability	Important	7.1	No	No	RCE
CVE-2021-34520	Microsoft SharePoint Server Remote Code Execution Vulnerability	Important	8.1	No	No	RCE
CVE-2021-34517	Microsoft SharePoint Server Spoofing Vulnerability	Important	5.3	No	No	Spoofing
CVE-2021-34479	Microsoft Visual Studio Spoofing Vulnerability	Important	7.8	No	No	Spoofing
CVE-2021-34441	Microsoft Windows Media Foundation Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2021-34452	Microsoft Word Remote Code Execution Vulnerability	Important	7.8	No	No	RCE

CVE	Title	Severity	CVSS	Public	Exploited	Type
CVE-2021-33767	Open Enclave SDK Elevation of Privilege Vulnerability	Important	8.2	No	No	EoP
CVE-2021-31984	Power BI Remote Code Execution Vulnerability	Important	7.6	No	No	RCE
CVE-2021-34521	Raw Image Extension Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2021-33751	Storage Spaces Controller Elevation of Privilege Vulnerability	Important	7	No	No	EoP
CVE-2021-34460	Storage Spaces Controller Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-34510	Storage Spaces Controller Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-34512	Storage Spaces Controller Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-34513	Storage Spaces Controller Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-34509	Storage Spaces Controller Information Disclosure Vulnerability	Important	5.5	No	No	Info
CVE-2021-34477	Visual Studio Code .NET Runtime Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-34528	Visual Studio Code Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2021-34529	Visual Studio Code Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2021-34449	Win32k Elevation of Privilege Vulnerability	Important	7	No	No	EoP

CVE	Title	Severity	CVSS	Public	Exploited	Type
CVE-2021-34516	Win32k Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-34491	Win32k Information Disclosure Vulnerability	Important	5.5	No	No	Info
CVE-2021-34504	Windows Address Book Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2021-33785	Windows AF_UNIX Socket Provider Denial of Service Vulnerability	Important	7.5	No	No	DoS
CVE-2021-34459	Windows AppContainer Elevation Of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-34462	Windows AppX Deployment Extensions Elevation of Privilege Vulnerability	Important	7	No	No	EoP
CVE-2021-33782	Windows Authenticode Spoofing Vulnerability	Important	5.5	No	No	Spoofing
CVE-2021-33784	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-34488	Windows Console Driver Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-34461	Windows Container Isolation FS Filter Driver Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-33759	Windows Desktop Bridge Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-33745	Windows DNS Server Denial of Service Vulnerability	Important	6.5	No	No	DoS
CVE-2021-34442	Windows DNS Server Denial of Service Vulnerability	Important	7.5	No	No	DoS

CVE	Title	Severity	CVSS	Public	Exploited	Type
CVE-2021-34444	Windows DNS Server Denial of Service Vulnerability	Important	6.5	No	No	DoS
CVE-2021-34499	Windows DNS Server Denial of Service Vulnerability	Important	6.5	No	No	DoS
CVE-2021-33746	Windows DNS Server Remote Code Execution Vulnerability	Important	8	No	No	RCE
CVE-2021-33754	Windows DNS Server Remote Code Execution Vulnerability	Important	8	No	No	RCE
CVE-2021-33780	Windows DNS Server Remote Code Execution Vulnerability	Important	8.8	No	No	RCE
CVE-2021-34525	Windows DNS Server Remote Code Execution Vulnerability	Important	8.8	No	No	RCE
CVE-2021-33749	Windows DNS Snap-in Remote Code Execution Vulnerability	Important	8.8	No	No	RCE
CVE-2021-33750	Windows DNS Snap-in Remote Code Execution Vulnerability	Important	8.8	No	No	RCE
CVE-2021-33752	Windows DNS Snap-in Remote Code Execution Vulnerability	Important	8.8	No	No	RCE
CVE-2021-33756	Windows DNS Snap-in Remote Code Execution Vulnerability	Important	8.8	No	No	RCE
CVE-2021-33774	Windows Event Tracing Elevation of Privilege Vulnerability	Important	7	No	No	EoP
CVE-2021-34455	Windows File History Service Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-34438	Windows Font Driver Host Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2021-34498	Windows GDI Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP

CVE	Title	Severity	CVSS	Public	Exploited	Type
CVE-2021-34496	Windows GDI Information Disclosure Vulnerability	Important	5.5	No	No	Info
CVE-2021-34466	Windows Hello Security Feature Bypass Vulnerability	Important	5.7	No	No	SFB
CVE-2021-34446	Windows HTML Platform Security Feature Bypass Vulnerability	Important	8	No	No	SFB
CVE-2021-33755	Windows Hyper-V Denial of Service Vulnerability	Important	6.3	No	No	DoS
CVE-2021-33758	Windows Hyper-V Denial of Service Vulnerability	Important	7.7	No	No	DoS
CVE-2021-34511	Windows Installer Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-33765	Windows Installer Spoofing Vulnerability	Important	6.2	No	No	Spoofing
CVE-2021-31961	Windows InstallService Elevation of Privilege Vulnerability	Important	6.1	No	No	EoP
CVE-2021-34514	Windows Kernel Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-34500	Windows Kernel Memory Information Disclosure Vulnerability	Important	6.3	No	No	Info
CVE-2021-34508	Windows Kernel Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2021-33764	Windows Key Distribution Center Information Disclosure Vulnerability	Important	5.9	No	No	Info
CVE-2021-33788	Windows LSA Denial of Service Vulnerability	Important	7.5	No	No	DoS
CVE-2021-33786	Windows LSA Security Feature Bypass Vulnerability	Important	8.1	No	No	SFB

CVE	Title	Severity	CVSS	Public	Exploited	Type
CVE-2021-34447	Windows MSHTML Platform Remote Code Execution Vulnerability	Important	6.8	No	No	RCE
CVE-2021-34493	Windows Partition Management Driver Elevation of Privilege Vulnerability	Important	6.7	No	No	EoP
CVE-2021-33743	Windows Projected File System Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-33761	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-33773	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-34445	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-34456	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-33763	Windows Remote Access Connection Manager Information Disclosure Vulnerability	Important	5.5	No	No	Info
CVE-2021-34454	Windows Remote Access Connection Manager Information Disclosure Vulnerability	Important	5.5	No	No	Info
CVE-2021-34457	Windows Remote Access Connection Manager Information Disclosure Vulnerability	Important	5.5	No	No	Info

CVE	Title	Severity	CVSS	Public	Exploited	Type
CVE-2021-34507	Windows Remote Assistance Information Disclosure Vulnerability	Important	6.5	No	No	Info
CVE-2021-33744	Windows Secure Kernel Mode Security Feature Bypass Vulnerability	Important	5.3	No	No	SFB
CVE-2021-33757	Windows Security Account Manager Remote Protocol Security Feature Bypass Vulnerability	Important	5.3	No	No	SFB
CVE-2021-33783	Windows SMB Information Disclosure Vulnerability	Important	5.5	No	No	Info
CVE-2021-31183	Windows TCP/IP Driver Denial of Service Vulnerability	Important	7.5	No	No	DoS
CVE-2021-33772	Windows TCP/IP Driver Denial of Service Vulnerability	Important	7.5	No	No	DoS
CVE-2021-34490	Windows TCP/IP Driver Denial of Service Vulnerability	Important	7.5	No	No	DoS
CVE-2021-34519	Microsoft SharePoint Server Information Disclosure Vulnerability	Moderate	5.3	No	No	Info

References

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

Adobe Security Bulletins and Advisories
https://helpx.adobe.com/security/security-bulletin.html

Intel Product Security Center Advisories
https://www.intel.com/content/www/us/en/security-center/default.html

Microsoft July 2021 Security Updates
https://msrc.microsoft.com/update-guide/releaseNote/2021-Jul

Windows 10 cumulative updates KB5004237 & KB5004245 released
https://www.bleepingcomputer.com/news/microsoft/windows-10-cumulative-updates-kb5004237-and-kb5004245-released/

Microsoft Patch Tuesday for July 2021 — Snort rules and prominent vulnerabilities
https://blog.talosintelligence.com/2021/07/microsoft-patch-tuesday-for-july-2021.html

SAP Releases July 2021 Security Updates
https://us-cert.cisa.gov/ncas/current-activity/2021/07/13/sap-releases-july-2021-security-updates

Microsoft Crushes 116 Bugs, Three Actively Exploited
https://threatpost.com/microsoft-crushes-116-bugs/167764/

Microsoft July 2021 Patch Tuesday fixes 9 zero-days, 117 flaws
https://www.bleepingcomputer.com/news/microsoft/microsoft-july-2021-patch-tuesday-fixes-9-zero-days-117-flaws/

Panoply of critical patches in July updates require quick action
https://news.sophos.com/en-us/2021/07/13/panoply-of-critical-patches-in-july-updates-require-quick-action/

Windows 10 printing issues fixed by July Patch Tuesday update
https://www.bleepingcomputer.com/news/microsoft/windows-10-printing-issues-fixed-by-july-patch-tuesday-update/

Microsoft Patch Tuesday, July 2021 Edition
https://krebsonsecurity.com/2021/07/microsoft-patch-tuesday-july-2021-edition/

Microsoft Patches 3 Windows Zero-Days Amid 117 CVEs
https://beta.darkreading.com/vulnerabilities-threats/microsoft-patches-3-windows-zero-days-amid-117-cves

Mozilla Releases Security Updates for Firefox
https://us-cert.cisa.gov/ncas/current-activity/2021/07/13/mozilla-releases-security-updates-firefox

Apple releases fix for iOS and macOS zero-day, 13th this year
https://therecord.media/apple-releases-fix-for-ios-and-macos-zero-day-13th-this-year/

Adobe Releases Security Updates for Multiple Products
https://us-cert.cisa.gov/ncas/current-activity/2021/07/13/adobe-releases-security-updates-multiple-products

Apache Releases Security Advisory for Tomcat
https://us-cert.cisa.gov/ncas/current-activity/2021/07/13/apache-releases-security-advisory-tomcat

VMware Releases Security Update
https://us-cert.cisa.gov/ncas/current-activity/2021/07/13/vmware-releases-security-update

Citrix Releases Security Updates for Virtual Apps and Desktops
https://us-cert.cisa.gov/ncas/current-activity/2021/07/13/citrix-releases-security-updates-virtual-apps-and-desktops

HC3: Monthly Cybersecurity Vulnerability Bulletin

August 18, 2021 TLP: White Report: 202108180830

Contact Information

If you have any additional questions, please contact us at HC3@hhs.gov.

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