HC3: Monthly Cybersecurity Vulnerability Bulletin

September 7, 2021 TLP: White Report: 202109071300

August 2021 Cybersecurity News of Interest to the Health Sector

- RiskBased Security released their 2021 Mid-Year Data Breach Report in August. In that research, they identified 1,767 publicly reported breaches in the first six months of 2021, which represented a 24% decline compared to the same period last year and was the fewest breaches they had identified since their 2014 report. They found that 18.8 billion records were exposed year to date, a 32% decline as compared to 27.8 billion records exposed in the first half of 2020. Of the 1,767 breaches identified, the majority – 1201 – were caused by a cyberattack. The healthcare sector remained the most targeted and breached industry accounting for 238 of breaches so far this year.
- A denial-of-service vulnerability has been found by SentinelOne in Cobalt Strike – a legitimate tool used by pen testers and red teams to identify security gaps in an organizations information infrastructure. However, it is also frequently used for malicious purposes, as part of a cyberattack. HC3 has observed denial-of-service to target healthcare organizations over the last six to eight months. This vulnerability allows an attacker to register fake beacons with a Cobalt Strike server which can crash the server by exhausting available memory; therefore, no longer receiving beacons and prevents new beaconing instances from being installed on compromised systems. This is noteworthy not because it's expected to have an impact on legitimate red team/pen testing activities but because it's a potential means by which to disrupt command and control for an ongoing cyber attack. However, many sophisticated threat actors are expected to be aware of this and ensure they are working with the latest version of Cobalt Strike, which was impacted by this vulnerability. This vulnerability is tracked as CVE-2021-36798 and has been called HotCobalt.
- The company Critical Insight released their Healthcare Breach report for the first half of 2021 in August. The number of breaches in the first half of 2021 are as high as they have been for any six-month period since 2018, excluding the second half of last year in 2020, which has a spike due to a single, large breach. According to their report, breaches have been steadily increasing over time and have almost doubled – increased 77% - in the last three years. Critical Insight also found outpatient facilities, especially family medicine and specialty clinics, to be heavily targeted. Outpatient facilities were breached almost as much as hospitals. Finally, they noted that business associates were the cause of 43% of all healthcare breaches, which continues a 3-year increasing trend.
- The FBI released a report on a cybercriminal gang called the OnePercent Group. This was the first time the FBI has released an alert on a ransomware affiliate. They have been known to operate since at least November 2020. The OnePercent Group is known to use phishing as their primary attack vector, IcedID and Cobalt Strike as later stage malware for further compromise and lateral movement and they like to contact their victims via phone or e-mail, vice leaving a ransom note. To a lesser extent, they also use PowerShell, Mimikatz, Rclone, BetterSafetykatz and SharpSploit. They also are believed to have connection with the REvil operators as well as Egregor.
- The cybersecurity company Armis did some research on pneumatic tube systems (PTS) produced by TransLogic. A PTS is a series of tubes, usually in a single building but sometimes between several buildings that allow you to move small objects around quickly. They are often used in hospitals to move things such as lab samples, blood, tissue or medication from one part of the medical facility to another. TransLogic PTS are believed to be present in more than 2,300 hospitals in North America. That research conducted by Armis revealed that an unauthenticated attacker could gain full control over TransLogic pneumatic tube systems that are connected to the internet and then compromise the entire tube network of a target hospital. Armis identified nine vulnerabilities which are being collectively referred to as PwnedPiper. They cover issues such as password leakage, remote code execution, denial-of-service, and full device compromise. For these nine vulnerabilities, all but one of them can be addressed by installing the latest firmware. Armis developed Snort signatures for any healthcare organization that can't install the firmware but is running Snort. HC3 developed a sector alert on the PwnedPiper vulnerabilities which can be found at: https://www.hhs.gov/sites/default/files/pwnedpiper-sector-alert-tlpwhite.pdf

HC3: Monthly Cybersecurity Vulnerability Bulletin

September 7, 2021 TLP: White Report: 202109071300

Vulnerabilities of Interest to the Health Sector for the Month of August

Executive Summary

In August 2021, vulnerabilities in common information systems relevant to the healthcare sector have been released which require prioritized attention. This includes the monthly Patch Tuesday vulnerabilities – released by several vendors on the second Tuesday of each month – along with mitigation steps and/or patches as they are developed. Vulnerabilities for this month are from Microsoft, McAfee, Adobe, Blackberry QNX Intel, Cisco, Citrix, SAP, and VMWare. Vulnerabilities should be considered for patching with special consideration to each vulnerability criticality category against the risk management posture of the organization. Accountability, proper inventory management and asset tracking are vital to an effective patch management program.

Report

MICROSOFT

Microsoft released fixes for 44 vulnerabilities in the company's firmware and software: Microsoft Windows and Windows components, Office, .NET Core and Visual Studio, Windows Defender, Windows Update and Update Assistant, Azure, and Microsoft Dynamics. While this is the fewest amount of vulnerabilities Microsoft has patched in a month since December 2019, there was a noticeably high percentage of critical vulnerabilities. Of these 44 vulnerabilities, seven were classified as Critical and 37 as Important. In terms of categories, they can be broken down as: 13 remote code execution, eight information disclosure, two denial of service, and four are spoofing vulnerabilities. You can find additional information about the non-security Windows updates, Windows 10 KB5005033 & KB5005031 cumulative updates here.

These updates include three fixes for zero-day vulnerabilities that were actively exploited or publicly disclosed, like PrintNightmare and PetitPotam. Microsoft has released security updates for two eagerly anticipated zero-day vulnerabilities that were discovered over the past month. One of the security updates fixes the PrintNightmare vulnerabilities that allow threat actors to gain SYSTEM level privileges simply by connecting to a remote print server under their control. Microsoft has fixed this vulnerability by requiring users have administrative privileges to install printer drivers using the Point and Print Windows feature. You can find more detailed information about the PrintNightmare vulnerability and the Point and Print mitigations in this dedicated article.

Microsoft also fixed the PetitPotam NTLM relay attack vector that uses the MS-EFSRPC API to force a device to negotiate with a remote relay server under an attacker's control. A threat actor with low privileges could use this attack to take over a domain controller and thus the entire Windows domain. Microsoft has released security updates for three zero-day vulnerabilities, with one actively exploited in the wild. Microsoft classifies a vulnerability as a zero-day if it is publicly disclosed or actively exploited with no official security updates or released. The two publicly disclosed, but not actively exploited, zero-day vulnerabilities are:

- CVE-2021-36936 - Windows Print Spooler Remote Code Execution Vulnerability
- CVE-2021-36942 - Windows LSA Spoofing Vulnerability

The CVE-2021-36942 vulnerability is associated with the PetitPotam NTLM relay attack vector that allows the take over of domain controllers. In addition to this, one actively exploited elevation of privileges vulnerability was discovered by the Microsoft Security Response Center (MSRC) and Microsoft Threat Intelligence Center (MSTIC).

- CVE-2021-36948 - Windows Update Medic Service Elevation of Privilege Vulnerability

At this time, it is not known how threat actors used this vulnerability in attacks. HC3 recommends applying patches and testing immediately. You can learn more on how to manually install these updates here.

McAFEE

CVE-2021-34535 is a critical vulnerability that was identified by McAfee. It is a remote code execution flaw in the Remote Desktop client software, observed in mstscax.dll, which is used by Microsoft's built-in remote desktop protocol (RDP) client (mstsc.exe). The vulnerability is an integer overflow due to an attacker-controllable payload size field, which ultimately leads to a heap buffer overflow during memory allocation. The vulnerability can be triggered via the RDP Video Redirection Virtual Channel Extension feature [MS-RDPEV], which is typically associated with port 3389, and is contained inside of compressed UDP payload and encrypted RDP using TLS. As always, testing is recommended prior to patching.

Microsoft's Hyper-V Manager software also uses mstscax.dll where the vulnerable function resides. When using "Enhanced Session Mode" (enabled by default in Hyper-V Manager), the process vmconnect.exe loads mstscax.dll. Testing confirms that triggering the vulnerability from inside a Hyper-V Windows 10 image will crash vmconnect.exe on the host which means it is subject to guest-to-host escapes using the vulnerability. (Hyper-V is disabled by Default on Windows 10). For RDP security best practices please check here.

ADOBE

Adobe released two patches addressing 29 CVEs in Adobe Connect and Magento. The update for Connect is rated Important and fixes a single security feature bypass and two cross-site scripting bugs. The Critical-rated patch for Magento fixes a wide range of bugs, the worst of which could allow remote code execution. None of the bugs fixed this month by Adobe are listed as publicly known or under active attack at the time of release. The complete list of Adobe Products receiving security updates today and the number of fixed vulnerabilities are below:

- APSB21-64 Security updates available for Magento
- APSB21-66 Security update available for Adobe Connect

Almost all Critical vulnerabilities could lead to arbitrary code execution, allowing threat actors to execute commands on vulnerable computers. Out of the Adobe security updates released, Magento has the most fixes, with 26 vulnerabilities. Of particular concern are ten pre-authentication vulnerabilities in Magento that can be exploited without logging into the site. Some of these preauth vulnerabilities are remote code execution and security bypasses, allowing a threat actor to control a site and it's server. HC3 recommends installing updates immediately. While there were no known actively exploited zero-day vulnerabilities, Adobe advises customers to update to the latest versions as soon as possible. This urgency is because threat actors can compare older versions of the software with the patched versions to determine what code is vulnerable and create exploits to target these vulnerabilities.

In most cases, users can update their software by using the auto-update feature of the product using the following steps:

- Go to **Help** > **Check for Updates**.
- The update installers can be downloaded from Adobe's Download Center.
- Let the products update automatically, without requiring user intervention, when updates are detected.

For Magento updates, you will need to download the appropriate patches and install them manually. If the new update is not available via auto update, you can check the security bulletins linked above for the latest download links.

HC3: Monthly Cybersecurity Vulnerability Bulletin

September 7, 2021 TLP: White Report: 202109071300

Blackberry QNX

CISA issued an Alert on devices incorporating older versions of multiple BlackBerry QNX products affected by a BadAlloc vulnerability—CVE-2021-22156. A malicious actor could exploit this vulnerability to take control of an affected system or cause a denial-of-service condition. CISA is not aware of active exploitation of this vulnerability currently. According to CISA, devices incorporating older versions of BlackBerry QNX products support critical infrastructure and national critical functions and organizations whose devices use affected QNX-based systems are strongly urged to immediately apply the mitigations provided in CISA Alert AA21-229A and Blackberry Advisory QNX-2021-001

INTEL

Intel has released security updates to address vulnerabilities in multiple products. An attacker could exploit some of these vulnerabilities to take control of an affected system. Administrators and users are advised to review the following Intel advisories and apply the necessary updates:

- NUC 9 Extreme Laptop Kits Advisory INTEL-SA-00553
- NUC Pro Chassis Element Driver Advisory INTEL-SA-00543
- Ethernet Linux Driver Advisory INTEL-SA-00515
- Optane PMem Advisory INTEL-SA-00512
- Graphics Drivers Advisory INTEL-SA-00508
- Ethernet Adapters 800 Series Advisory INTEL-SA-00479

A potential security vulnerability in some Intel® NUC 9 Extreme Laptop Kits may allow escalation of privilege. Intel is releasing software updates to mitigate this potential vulnerability. HC3 recommends updating the Intel® NUC 9 Extreme Laptop software driver kit to version 2.2.0.20 or later.

Vulnerability Details: CVEID: CVE-2021-0196 allows improper access control in kernel mode driver for some Intel(R) NUC 9 Extreme Laptop Kits before version 2.2.0.20 may allow an authenticated user to potentially enable escalation of privilege via local access.

CVSS Base Score: 7.8 High | *CVSS Vector:* CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

Affected Products: Intel® NUC 9 Extreme Laptop Kit - LAPQC71A | Intel® NUC 9 Extreme Laptop Kit - LAPQC71B | Intel® NUC 9 Extreme Laptop Kit - LAPQC71C | Intel® NUC 9 Extreme Laptop Kit - LAPQC71D
Updates are available for download here.

CISCO

Cisco released security updates for several products this month and from the vulnerabilities listed, 20 were categorized as Medium, four Critical, and 12 as High.

Cisco Application Policy Infrastructure Controller Arbitrary File Read and Write Vulnerability	Critical	CVE-2021-1577	2021 Aug 25	1.0
BlackBerry QNX-2021-001 Vulnerability Affecting Cisco Products: August 2021	Critical	CVE-2021-22156	2021 Aug 25	1.4
Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers Remote Command Execution and Denial of Service Vulnerability	Critical	CVE-2021-34730	2021 Aug 18	1.0
Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers Web Management Vulnerabilities	Critical	CVE-2021-1609 CVE-2021-1610	2021 Aug 04	1.0

Multiple Vulnerabilities in OpenSSL Affecting Cisco Products: March 2021	High	CVE-2021-3449 CVE-2021-3450	2021 Aug 30	1.19
Cisco NX-OS Software VXLAN OAM (NGOAM) Denial of Service Vulnerability	High	CVE-2021-1587	2021 Aug 25	1.0
Cisco NX-OS Software MPLS OAM Denial of Service Vulnerability	High	CVE-2021-1588	2021 Aug 25	1.0
Cisco Nexus 9000 Series Fabric Switches ACI Mode Multi-Pod and Multi-Site TCP Denial of Service Vulnerability	High	CVE-2021-1586	2021 Aug 25	1.0
Cisco Nexus 9000 Series Fabric Switches ACI Mode Queue Wedge Denial of Service Vulnerability	High	CVE-2021-1523	2021 Aug 25	1.0
Cisco Application Policy Infrastructure Controller Privilege Escalation Vulnerability	High	CVE-2021-1578	2021 Aug 25	1.0
Cisco Application Policy Infrastructure Controller App Privilege Escalation Vulnerability	High	CVE-2021-1579	2021 Aug 25	1.0
Cisco Small Business RV160 and RV260 Series VPN Routers Remote Command Execution Vulnerability	High	CVE-2021-1602	2021 Aug 04	1.0
Cisco Packet Tracer for Windows DLL Injection Vulnerability	High	CVE-2021-1593	2021 Aug 04	1.0
Cisco Network Services Orchestrator CLI Secure Shell Server Privilege Escalation Vulnerability	High	CVE-2021-1572	2021 Aug 04	1.0
ConfD CLI Secure Shell Server Privilege Escalation Vulnerability	High	CVE-2021-1572	2021 Aug 04	1.0
Cisco Small Business RV Series Routers Link Layer Discovery Protocol Vulnerabilities	High	CVE-2021-1251 CVE-2021-1308 ...	2021 Aug 04	1.2

CITRIX

Citrix has released a security update addressing a vulnerability that impacts Citrix ShareFile storage zones controller. This vulnerability allows an attacker to exploit a compromised system and obtain access to sensitive data. It is extremely important for users and administrators to review Citrix Security Bulletin CTX322787 and apply the necessary update immediately.

Customers are only affected by this issue if they previously selected “Enable Encryption” in the ShareFile storage zones controller configuration page and did not re-select this setting after running the CTX269106 mitigation tool. ShareFile customers who have not run the CTX269106 mitigation tool or who re-selected “Enable Encryption” immediately after running the tool are unaffected by this issue. Customers using Citrix ShareFile storage zones controller 5.10.1 and above or 5.11.18 and above can check if they are affected by this issue by viewing the EncryptionServiceSettings file in the StorageLocation. If IsEncryptionNeeded is set to True then the storage zones controller is affected by this issue. Affected customers using 5.11.19 or above who log-in to the ShareFile storage zones controller configuration page will also be presented with a pop-up which informs them they are affected by this issue.

CVE-ID	Description	Type	Pre-requisites
CVE-2021-22932	File encryption is disabled after running CTX269106 mitigation tool	CWE-312: Cleartext Storage of Sensitive Information	Access to an affected customer-managed ShareFile storage zone

Customers who are unsure if they have been affected or who have previously run the CTX269106 mitigation tool are recommended to check if they are affected by this issue by following the steps above. Citrix strongly recommends

affected customers address this issue as soon as possible by first upgrading to ShareFile storage zones controller 5.11.19 or later and then running the background encryption task to ensure any files which were not encrypted due to this issue become encrypted. More information on this process is available at https://citrix.sharefile.com/d-s09aed5d7e9ad4e89b97be38162edd201. The latest versions of Citrix ShareFile storage zones controller are available on the Citrix website.

SAP

SAP released 14 Security Notes on Patch Tuesday. There was also one update to a previously released Patch Tuesday Security Note. SAP released these security updates to address vulnerabilities impacting multiple products which are dangerous as an attacker could exploit these vulnerabilities to take control of an affected system. Administrators and users should review SAP Security Notes for August 2021 and apply the necessary updates immediately. HC3 recommends customers visit the Support Portal and apply patches on a priority to protect their SAP landscape.

The following are considered high priority:

3073681	[CVE-2021-33702] **Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver Enterprise Portal** Product - SAP NetWeaver Enterprise Portal, Versions - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50	High	8.3
3072920	[CVE-2021-33703] **Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver Enterprise Portal** Product - SAP NetWeaver Enterprise Portal (Application Extensions), Versions - 7.30, 7.31, 7.40, 7.50	High	8.3
3074844	[CVE-2021-33705] **Server-Side Request Forgery (SSRF) vulnerability in SAP NetWeaver Enterprise Portal** Product - SAP NetWeaver Enterprise Portal, Versions - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50	High	8.1
3067219	[CVE-2021-33699] **Task Hijacking in SAP Fiori Client Native Mobile for Android** Product - SAP Fiori Client Native Mobile for Android, Version - 3.2	High	7.6
3073325	[CVE-2021-33700] **Missing Authentication check in SAP Business One** Product - SAP Business One, Version - 10.0	High	7

VMWARE

VMware released security updates for VMware Workspace ONE. On August 24, 2021, one Advisory ID VMSA-2021-000.4.2 was categorized as a Critical vulnerability. VMware vRealize Operations updates address Server-Side Request Forgery and Arbitrary File Write vulnerabilities (CVE-2021-21975, CVE-2021-21983). In addition to this, there were three Advisory ID's (VMSA-2021-0018, VMSA-2021-0016.1, VMSA-2021-0014.1), categorized as Important vulnerabilities. The critical Advisory ID VMSA-2021-000.4.2 impacts the following products: VMware vRealize Operations, VMware Cloud Foundation, and vRealize Suite Lifecycle Manager.

CVE-2021-21975 - Server Side Request Forgery in vRealize Operations Manager API: The vRealize Operations Manager API contains a Server Side Request Forgery. VMware considers this issue to be of 'Important' severity with a maximum CVSSv3 base score of 8.6. An attacker with network access to the vRealize Operations Manager API has the ability to perform a Server Side Request Forgery attack to steal administrative credentials.

CVE-2021-21983 - Arbitrary file write vulnerability in vRealize Operations Manager API: The vRealize Operations Manager API contains an arbitrary file write vulnerability. VMware has identified this issue's severity as

'Important' with a maximum CVSSv3 base score of 7.2. An authenticated threat actor with network access to the vRealize Operations Manager API can write files to arbitrary locations on the underlying photon operating system. To remediate CVE-2021-21975 and CVE-2021-21983, apply updates listed in the 'Fixed Version' column of the 'Response Matrix' (toward end of bulletin) to impacted deployments. Workarounds are listed there as well.

QNAP

Network-attached storage (NAS) maker QNAP is investigating and working on security updates to address remote code execution (RCE) and denial-of-service (DoS) vulnerabilities patched by OpenSSL. The security flaws tracked as CVE-2021-3711 and CVE-2021-3712, impact QNAP NAS device running QTS, QuTS hero, QuTScloud, and HBS 3 Hybrid Backup Sync (a backup and disaster recovery app), according to advisories [1, 2].The heap-based buffer overflow in the SM2 cryptographic algorithm behind CVE-2021-3711 would likely lead to crashes but can also be abused by attackers for arbitrary code execution.

The CVE-2021-3712 vulnerability is caused by a read buffer overrun weakness while processing ASN.1 strings. Threat actors can exploit it to crash vulnerable apps or gain access to private memory contents such as private keys or sensitive data. If successfully exploited these vulnerabilities will give threat actors remote access to memory data without authorization, trigger DoS states, or run arbitrary code with the permissions of the user running the HBS 3 app. OpenSSL 1.1.1l has been published to address these flaws however QNAP has not provide an estimated time of arrival for incoming security updates. The company said they "will release security updates and provide further information as soon as possible."

THROUGHTEK KALAY P2P SDK: CVE-2021-28732 ICS ADVISORY (ICSA-21-229-01)

CISA released an ICS advisory for (ISCA-21-229-01) and CVE-2021-28372. Successful exploitation of this vulnerability could permit remote code execution and unauthorized access to sensitive information, such as camera audio/video feeds. At this time, CISA has not identified active exploitation of this vulnerability. For current Activity Alert CISA Releases Security Advisory for ThroughTek Kalay P2P visit CISA's website.

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

CVE	Title	Severity	CVSS	Public	Exploited	Type
CVE-2021-36948	Windows Update Medic Service Elevation of Privilege Vulnerability	Important	7.8	No	Yes	EoP
CVE-2021-36936	Windows Print Spooler Remote Code Execution Vulnerability	Critical	8.8	Yes	No	RCE
CVE-2021-36942	Windows LSA Spoofing Vulnerability	Important	9.8	Yes	No	Spoofing
CVE-2021-34535	Remote Desktop Client Remote Code Execution Vulnerability	Critical	9.9	No	No	RCE
CVE-2021-34480	Scripting Engine Memory Corruption Vulnerability	Critical	6.8	No	No	RCE
CVE-2021-34530	Windows Graphics Component Remote Code Execution Vulnerability	Critical	7.8	No	No	RCE
CVE-2021-34534	Windows MSHTML Platform Remote Code Execution Vulnerability	Critical	6.8	No	No	RCE
CVE-2021-26432	Windows Services for NFS ONCRPC XDR Driver Remote Code Execution Vulnerability	Critical	9.8	No	No	RCE
CVE-2021-26424	Windows TCP/IP Remote Code Execution Vulnerability	Critical	9.9	No	No	RCE

HC3: Monthly Cybersecurity Vulnerability Bulletin

September 7, 2021 TLP: White Report: 202109071300

CVE	Title	Severity	CVSS	Public	Exploited	Type
CVE-2021-26423	.NET Core and Visual Studio Denial of Service Vulnerability	Important	7.5	No	No	DoS
CVE-2021-34485	.NET Core and Visual Studio Information Disclosure Vulnerability	Important	5	No	No	Info
CVE-2021-34532	ASP.NET Core and Visual Studio Information Disclosure Vulnerability	Important	5.5	No	No	Info
CVE-2021-33762	Azure CycleCloud Elevation of Privilege Vulnerability	Important	7	No	No	EoP
CVE-2021-36943	Azure CycleCloud Elevation of Privilege Vulnerability	Important	4	No	No	EoP
CVE-2021-26430	Azure Sphere Denial of Service Vulnerability	Important	6	No	No	DoS
CVE-2021-26429	Azure Sphere Elevation of Privilege Vulnerability	Important	7.7	No	No	EoP
CVE-2021-26428	Azure Sphere Information Disclosure Vulnerability	Important	4.4	No	No	Info
CVE-2021-36949	Microsoft Azure Active Directory Connect Authentication Bypass Vulnerability	Important	7.1	No	No	SFB
CVE-2021-36950	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	Important	5.4	No	No	XSS
CVE-2021-34524	Microsoft Dynamics 365 (on-premises) Remote Code Execution Vulnerability	Important	8.1	No	No	RCE
CVE-2021-36946	Microsoft Dynamics Business Central Cross-site Scripting Vulnerability	Important	5.4	No	No	XSS
CVE-2021-34478	Microsoft Office Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2021-36940	Microsoft SharePoint Server Spoofing Vulnerability	Important	7.6	No	No	Spoofing
CVE-2021-34471	Microsoft Windows Defender Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-36941	Microsoft Word Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2021-34536	Storage Spaces Controller Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-36945	Windows 10 Update Assistant Elevation of Privilege Vulnerability	Important	7.3	No	No	EoP
CVE-2021-34537	Windows Bluetooth Service Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-36938	Windows Cryptographic Primitives Library Information Disclosure Vulnerability	Important	5.5	No	No	Info
CVE-2021-36927	Windows Digital TV Tuner device registration application Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-26425	Windows Event Tracing Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-34486	Windows Event Tracing Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-34487	Windows Event Tracing Elevation of Privilege Vulnerability	Important	7	No	No	EoP

HC3: Monthly Cybersecurity Vulnerability Bulletin

September 7, 2021 TLP: White Report: 202109071300

CVE	Title	Severity	CVSS	Public	Exploited	Type
CVE-2021-34533	Windows Graphics Component Font Parsing Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2021-36937	Windows Media MPEG-4 Video Decoder Remote Code Execution Vulnerability	Important	7.8	No	No	RCE
CVE-2021-34483	Windows Print Spooler Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-36947	Windows Print Spooler Remote Code Execution Vulnerability	Important	8.8	No	No	RCE
CVE-2021-26431	Windows Recovery Environment Agent Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-26433	Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability	Important	7.5	No	No	Info
CVE-2021-36926	Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability	Important	7.5	No	No	Info
CVE-2021-36932	Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability	Important	7.5	No	No	Info
CVE-2021-36933	Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability	Important	7.5	No	No	Info
CVE-2021-26426	Windows User Account Profile Picture Elevation of Privilege Vulnerability	Important	7	No	No	EoP
CVE-2021-34484	Windows User Profile Service Elevation of Privilege Vulnerability	Important	7.8	No	No	EoP
CVE-2021-30590	Chromium: CVE-2021-30590 Heap buffer overflow in Bookmarks	High	N/A	No	No	RCE
CVE-2021-30591	Chromium: CVE-2021-30591 Use after free in File System API	High	N/A	No	No	RCE
CVE-2021-30592	Chromium: CVE-2021-30592 Out of bounds write in Tab Groups	High	N/A	No	No	RCE
CVE-2021-30593	Chromium: CVE-2021-30593 Out of bounds read in Tab Strip	High	N/A	No	No	Info
CVE-2021-30594	Chromium: CVE-2021-30594 Use after free in Page Info UI	High	N/A	No	No	RCE
CVE-2021-30596	Chromium: CVE-2021-30596 Incorrect security UI in Navigation	Medium	N/A	No	No	SFB
CVE-2021-30597	Chromium: CVE-2021-30597 Use after free in Browser UI	Medium	N/A	No	No	RCE

This months table includes the Chromium updates for Edge. These vulnerabilities are listed with the severity as assigned by Google, which is different from the standard Microsoft nomenclature. Google does not assign a CVSS score, so none are listed in the table.

Appendix B – High-prioritized vulnerabilities (Source: CISA)

att -- xmill	A heap-based buffer overflow vulnerability exists in the XML Decompression DecodeTreeBlock functionality of AT&T Labs Xmill 0.7. Within `DecodeTreeBlock` which is called during the decompression of an XMI file, a UINT32 is loaded from the file and used as trusted input as the length of a buffer. An attacker can provide a malicious file to trigger this vulnerability.	2021-08-20	7.5	CVE-2021-21827 MISC
att -- xmill	A heap-based buffer overflow vulnerability exists in the XML Decompression DecodeTreeBlock functionality of AT&T Labs Xmill 0.7. In the default case of DecodeTreeBlock a label is created via CurPath::AddLabel in order to track the label for later reference. An attacker can provide a malicious file to trigger this vulnerability.	2021-08-20	7.5	CVE-2021-21828 MISC
bludit -- bludit	Unrestricted File Upload in Bludit v3.8.1 allows remote attackers to execute arbitrary code by uploading malicious files via the component 'bl-kereln/ajax/upload-logo.php'.	2021-08-20	7.5	CVE-2020-18879 MISC
edit_comments_project -- edit_comments	The Edit Comments WordPress plugin through 0.3 does not sanitise, validate or escape the jal_edit_comments GET parameter before using it in a SQL statement, leading to a SQL injection issue	2021-08-23	7.5	CVE-2021-24551 MISC MISC
netmodule -- nb800_firmware	Certain NetModule devices allow Limited Session Fixation via PHPSESSID. These models with firmware before 4.3.0.113, 4.4.0.111, and 4.5.0.105 are affected: NB800, NB1600, NB1601, NB1800, NB1810, NB2700, NB2710, NB2800, NB2810, NB3700, NB3701, NB3710, NB3711, NB3720, and NB3800.	2021-08-23	7.5	CVE-2021-39290 MISC MISC
nuishop -- nuishop	Nuishop v2.3 contains a SQL injection vulnerability in /goods/getGoodsListByConditions/.	2021-08-26	7.5	CVE-2020-20675 MISC
safecurl_project -- safecurl	SafeCurl before 0.9.2 has a DNS rebinding vulnerability.	2021-08-20	7.5	CVE-2020-36474 MISC MISC

gitlab -- gitlab	A verbose error message in GitLab EE affecting all versions since 12.2 could disclose the private email address of a user invited to a group	2021-08-23	4	CVE-2021-22249 CONFIRM MISC MISC
gitlab -- gitlab	A vulnerability was discovered in GitLab versions before 14.0.2, 13.12.6, 13.11.6. GitLab Webhook feature could be abused to perform denial of service attacks.	2021-08-20	4	CVE-2021-22246 MISC MISC CONFIRM
gitlab -- gitlab	Improper authorization on the pipelines page in GitLab CE/EE affecting all versions since 13.12 allowed unauthorized users to view some pipeline information for public projects that have access to pipelines restricted to members only	2021-08-23	5	CVE-2021-22248 CONFIRM MISC
gnome -- libgda	In GNOME libgda through 6.0.0, gda-web-provider.c does not enable TLS certificate verification on the SoupSessionSync objects it creates, leaving users vulnerable to network MITM attacks. NOTE: this is similar to CVE-2016-20011.	2021-08-22	4.3	CVE-2021-39359 MISC MISC
gnome -- libgfbgraph	In GNOME libgfbgraph through 0.2.4, gfbgraph-photo.c does not enable TLS certificate verification on the SoupSessionSync objects it creates, leaving users vulnerable to network MITM attacks. NOTE: this is similar to CVE-2016-20011.	2021-08-22	4.3	CVE-2021-39358 MISC MISC
google -- chrome	Use after free in WebRTC in Google Chrome prior to 92.0.4515.159 allowed an attacker who convinced a user to visit a malicious website to potentially exploit heap corruption via a crafted HTML page.	2021-08-26	6.8	CVE-2021-30602 MISC MISC
google -- chrome	Type confusion in V8 in Google Chrome prior to 92.0.4515.159 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	2021-08-26	6.8	CVE-2021-30598 MISC MISC
google -- chrome	Use after free in Browser UI in Google Chrome on Chrome prior to 92.0.4515.131 allowed a remote attacker to potentially exploit heap corruption via physical access to the device.	2021-08-26	4.6	CVE-2021-30597 MISC MISC
google -- chrome	Incorrect security UI in Navigation in Google Chrome on Android prior to 92.0.4515.131 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2021-08-26	4.3	CVE-2021-30596 MISC MISC
google -- chrome	Use after free in Extensions API in Google Chrome prior to 92.0.4515.159 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.	2021-08-26	6.8	CVE-2021-30601 MISC MISC
google -- chrome	Use after free in File System API in Google Chrome prior to 92.0.4515.131 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-08-26	6.8	CVE-2021-30591 MISC MISC
google -- chrome	Out of bounds write in Tab Groups in Google Chrome prior to 92.0.4515.131 allowed an attacker who convinced a user to install a malicious extension to perform an out of bounds memory write via a crafted HTML page.	2021-08-26	6.8	CVE-2021-30592 MISC MISC

HC3: Monthly Cybersecurity Vulnerability Bulletin

September 7, 2021 TLP: White Report: 202109071300

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- application_extension_platform	A vulnerability in the Universal Plug-and-Play (UPnP) service of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of incoming UPnP traffic. An attacker could exploit this vulnerability by sending a crafted UPnP request to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a DoS condition. Cisco has not released software updates that address this vulnerability.	2021-08-18	10	CVE-2021-34730 CISCO
dated_news_project -- dated_news	The dated_news (aka Dated News) extension through 5.1.1 for TYPO3 allows SQL Injection.	2021-08-13	7.5	CVE-2021-36789 MISC MISC
throughtek -- kalay_p2p_software_development_kit	ThroughTek's Kalay Platform 2.0 network allows an attacker to impersonate an arbitrary ThroughTek (TUTK) device given a valid 20-byte uniquely assigned identifier (UID). This could result in an attacker hijacking a victim's connection and forcing them into supplying credentials needed to access the victim TUTK device.	2021-08-17	7.6	CVE-2021-28372 MISC MISC MISC
google -- tensorflow	TensorFlow is an end-to-end open source platform for machine learning. In affected versions when running shape functions, some functions (such as `MutableHashTableShape`) produce extra output information in the form of a `ShapeAndType` struct. The shapes embedded in this struct are owned by an inference context that is cleaned up almost immediately; if the upstream code attempts to access this shape information, it can trigger a segfault. `ShapeRefiner` is mitigating this for normal output shapes by cloning them (and thus putting the newly created shape under ownership of an inference context that will not die), but we were not doing the same for shapes and types. This commit fixes that by doing similar logic on output shapes and types. We have patched the issue in GitHub commit ee119d4a498979525046fba1c3dd3f13a039fbb1. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.	2021-08-13	4.6	CVE-2021-37690 CONFIRM MISC
routes_project -- routes	The routes (aka Extbase Yaml Routes) extension before 2.1.1 for TYPO3, when CsrfTokenViewHelper is used, allows Sensitive Information Disclosure because a session identifier is unsafely present in HTML output.	2021-08-13	5	CVE-2021-36793 CONFIRM MISC

HC3: Monthly Cybersecurity Vulnerability Bulletin

September 7, 2021 TLP: White Report: 202109071300

The August 2021 Patch Tuesday Security Updates

Below is the complete list of resolved vulnerabilities and released advisories in the August 2021 Patch Tuesday updates. To access the full description of each vulnerability and the systems that it affects, you can view the full report here.

Tag	CVE ID	CVE Title	Severity
.NET Core & Visual Studio	CVE-2021-34485	.NET Core and Visual Studio Information Disclosure Vulnerability	Important
.NET Core & Visual Studio	CVE-2021-26423	.NET Core and Visual Studio Denial of Service Vulnerability	Important
ASP.NET Core & Visual Studio	CVE-2021-34532	ASP.NET Core and Visual Studio Information Disclosure Vulnerability	Important
Azure	CVE-2021-36943	Azure CycleCloud Elevation of Privilege Vulnerability	Important
Azure	CVE-2021-33762	Azure CycleCloud Elevation of Privilege Vulnerability	Important
Azure Sphere	CVE-2021-26428	Azure Sphere Information Disclosure Vulnerability	Important
Azure Sphere	CVE-2021-26430	Azure Sphere Denial of Service Vulnerability	Important
Azure Sphere	CVE-2021-26429	Azure Sphere Elevation of Privilege Vulnerability	Important
Microsoft Azure Active Directory Connect	CVE-2021-36949	Microsoft Azure Active Directory Connect Authentication Bypass Vulnerability	Important
Microsoft Dynamics	CVE-2021-36946	Microsoft Dynamics Business Central Cross-site Scripting Vulnerability	Important
Microsoft Dynamics	CVE-2021-36950	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	Important
Microsoft Dynamics	CVE-2021-34524	Microsoft Dynamics 365 (on-premises) Remote Code Execution Vulnerability	Important
Microsoft Edge (Chromium-based)	CVE-2021-30591	Chromium: CVE-2021-30591 Use after free in File System API	Unknown
Microsoft Edge (Chromium-based)	CVE-2021-30592	Chromium: CVE-2021-30592 Out of bounds write in Tab Groups	Unknown
Microsoft Edge (Chromium-based)	CVE-2021-30597	Chromium: CVE-2021-30597 Use after free in Browser UI	Unknown
Microsoft Edge (Chromium-based)	CVE-2021-30594	Chromium: CVE-2021-30594 Use after free in Page Info UI	Unknown
Microsoft Edge (Chromium-based)	CVE-2021-30596	Chromium: CVE-2021-30596 Incorrect security UI in Navigation	Unknown
Microsoft Edge (Chromium-based)	CVE-2021-30590	Chromium: CVE-2021-30590 Heap buffer overflow in Bookmarks	Unknown
Microsoft Edge (Chromium-based)	CVE-2021-30593	Chromium: CVE-2021-30593 Out of bounds read in Tab Strip	Unknown
Microsoft Graphics Component	CVE-2021-34530	Windows Graphics Component Remote Code Execution Vulnerability	Critical
Microsoft Graphics Component	CVE-2021-34533	Windows Graphics Component Font Parsing Remote Code Execution Vulnerability	Important
Microsoft Office	CVE-2021-34478	Microsoft Office Remote Code Execution Vulnerability	Important
Microsoft Office SharePoint	CVE-2021-36940	Microsoft SharePoint Server Spoofing Vulnerability	Important
Microsoft Office Word	CVE-2021-36941	Microsoft Word Remote Code Execution Vulnerability	Important
Microsoft Scripting Engine	CVE-2021-34480	Scripting Engine Memory Corruption Vulnerability	Critical
Remote Desktop Client	CVE-2021-34535	Remote Desktop Client Remote Code Execution Vulnerability	Critical

HC3: Monthly Cybersecurity Vulnerability Bulletin

September 7, 2021 TLP: White Report: 202109071300

Tag	CVE ID	CVE Title	Severity
Windows Bluetooth Service	CVE-2021-34537	Windows Bluetooth Driver Elevation of Privilege Vulnerability	Important
Windows Cryptographic Services	CVE-2021-36938	Windows Cryptographic Primitives Library Information Disclosure Vulnerability	Important
Windows Defender	CVE-2021-34471	Microsoft Windows Defender Elevation of Privilege Vulnerability	Important
Windows Event Tracing	CVE-2021-34486	Windows Event Tracing Elevation of Privilege Vulnerability	Important
Windows Event Tracing	CVE-2021-34487	Windows Event Tracing Elevation of Privilege Vulnerability	Important
Windows Event Tracing	CVE-2021-26425	Windows Event Tracing Elevation of Privilege Vulnerability	Important
Windows Media	CVE-2021-36927	Windows Digital TV Tuner device registration application Elevation of Privilege Vulnerability	Important
Windows MSHTML Platform	CVE-2021-34534	Windows MSHTML Platform Remote Code Execution Vulnerability	Critical
Windows NTLM	CVE-2021-36942	Windows LSA Spoofing Vulnerability	Important
Windows Print Spooler Components	CVE-2021-34483	Windows Print Spooler Elevation of Privilege Vulnerability	Important
Windows Print Spooler Components	CVE-2021-36947	Windows Print Spooler Remote Code Execution Vulnerability	Important
Windows Print Spooler Components	CVE-2021-36936	Windows Print Spooler Remote Code Execution Vulnerability	Critical
Windows Services for NFS ONCRPC XDR Driver	CVE-2021-36933	Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability	Important
Windows Services for NFS ONCRPC XDR Driver	CVE-2021-26433	Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability	Important
Windows Services for NFS ONCRPC XDR Driver	CVE-2021-36932	Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability	Important
Windows Services for NFS ONCRPC XDR Driver	CVE-2021-26432	Windows Services for NFS ONCRPC XDR Driver Remote Code Execution Vulnerability	Critical
Windows Services for NFS ONCRPC XDR Driver	CVE-2021-36926	Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability	Important
Windows Storage Spaces Controller	CVE-2021-34536	Storage Spaces Controller Elevation of Privilege Vulnerability	Important
Windows TCP/IP	CVE-2021-26424	Windows TCP/IP Remote Code Execution Vulnerability	Critical
Windows Update	CVE-2021-36948	Windows Update Medic Service Elevation of Privilege Vulnerability	Important
Windows Update Assistant	CVE-2021-36945	Windows 10 Update Assistant Elevation of Privilege Vulnerability	Important
Windows Update Assistant	CVE-2021-26431	Windows Recovery Environment Agent Elevation of Privilege Vulnerability	Important
Windows User Profile Service	CVE-2021-34484	Windows User Profile Service Elevation of Privilege Vulnerability	Important
Windows User Profile Service	CVE-2021-26426	Windows User Account Profile Picture Elevation of Privilege Vulnerability	Important

References

Adobe Fixes critical preauth vulnerabilities in Magento
https://www.bleepingcomputer.com/news/security/adobe-fixes-critical-preauth-vulnerabilities-in-magento/

Adobe Releases Security Updates for Multiple Products
https://us-cert.cisa.gov/ncas/current-activity/2021/08/10/adobe-releases-security-updates-multiple-products

Adobe Releases Multiple Security Updates
https://us-cert.cisa.gov/ncas/current-activity/2021/08/18/adobe-releases-multiple-security-updates

Apple Releases Security Update
https://us-cert.cisa.gov/ncas/current-activity/2021/08/17/apple-releases-security-update

BadAlloc Vulnerability Affecting BlackBerry QNX RTOS(Revised 8/23)
https://us-cert.cisa.gov/ncas/alerts/aa21-229a

Bulletin (SB21-235) – Vulnerability Summary for the Week of August 16, 2021
https://us-cert.cisa.gov/ncas/bulletins/sb21-235

CISA Releases Security Advisory for Swisslog Healthcare
https://us-cert.cisa.gov/ncas/current-activity/2021/08/03/cisa-releases-security-advisory-swisslog-healthcare

CISA: Bulletin (SB21-242) Vulnerability Summary for the Week of August 23, 2021
https://us-cert.cisa.gov/ncas/bulletins/sb21-242

Cisco Releases Security Updates
https://us-cert.cisa.gov/ncas/current-activity/2021/08/05/cisco-releases-security-updates

Cisco: Firewall manager RCE bug is a zero-day, patch incoming
https://www.bleepingcomputer.com/news/security/cisco-firewall-manager-rce-bug-is-a-zero-day-patch-incoming/

Cisco fixes critical, high severity pre-auth flaws in VPN routers
https://www.bleepingcomputer.com/news/security/cisco-fixes-critical-high-severity-pre-auth-flaws-in-vpn-routers/

Cisco Releases Security Updates for Multiple Products
https://us-cert.cisa.gov/ncas/current-activity/2021/08/19/cisco-releases-security-updates-multiple-products

Cisco Releases Security Updates for Multiple Products
https://us-cert.cisa.gov/ncas/current-activity/2021/08/26/cisco-releases-security-updates-multiple-products

Citrix Releases Security Update for ShareFile Storage Zones Controller
https://us-cert.cisa.gov/ncas/current-activity/2021/08/10/citrix-releases-security-update-sharefile-storage-zones-controller

Fortinet patches bug letting attackers takeover servers remotely
https://www.bleepingcomputer.com/news/security/fortinet-patches-bug-letting-attackers-takeover-servers-remotely/

Google Issues Warning For 2 Billion Chrome Users
https://www.forbes.com/sites/gordonkelly/2021/08/21/google-chrome-warning-high-security-hacks-upgrade-chrome-now/?sh=5f906c57eac2

Google Releases Security Updates for Chrome
https://us-cert.cisa.gov/ncas/current-activity/2021/08/04/google-releases-security-updates-chrome

Google Releases Security Updates for Chrome
https://us-cert.cisa.gov/ncas/current-activity/2021/08/18/google-releases-security-updates-chrome

Intel Releases Multiple Security Updates
https://us-cert.cisa.gov/ncas/current-activity/2021/08/10/intel-releases-multiple-security-updates

ISC Releases Security Advisory for BIND
https://us-cert.cisa.gov/ncas/current-activity/2021/08/19/isc-releases-security-advisory-bind

McAfee Enterprise - August 2021 Patch Tuesday - Critical RDP Vulnerabilities Continue to Proliferate
https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/critical-rdp-vulnerabilities-continue-to-proliferate/

Microsoft August 2021 Patch Tuesday fixes 3 zero-days, 44 flaws
https://www.bleepingcomputer.com/news/microsoft/microsoft-august-2021-patch-tuesday-fixes-3-zero-days-44-flaws/

Microsoft August 2021 Patch Tuesday vulnerability list
https://rawcdn.githack.com/campuscodi/Microsoft-Patch-Tuesday-Security-Reports/a5481bce61c205123065367dc9bf703dc9028a07/Reports/MSRC_CVEs2021-Aug.html

Microsoft Patch Tuesday for August 2021 — Snort rules and prominent vulnerabilities
https://blog.talosintelligence.com/2021/08/microsoft-patch-tuesday-for-august-2021.html

Microsoft Patch Tuesday, August 2021 Edition , Windows 10 KB5005033 & KB5005031 cumulative updates released
https://krebsonsecurity.com/2021/08/microsoft-patch-tuesday-august-2021-edition/

Microsoft August 2021 Security Updates
https://msrc.microsoft.com/update-guide/releaseNote/2021-Aug

Mozilla Releases Security Updates for Firefox
https://us-cert.cisa.gov/ncas/current-activity/2021/08/10/mozilla-releases-security-updates-firefox

Mozilla Releases Security Updates for Thunderbird
https://us-cert.cisa.gov/ncas/current-activity/2021/08/12/mozilla-releases-security-updates-thunderbird

Mozilla Releases Security Updates
https://us-cert.cisa.gov/ncas/current-activity/2021/08/18/mozilla-releases-security-updates

OpenSSL Releases Security Update
https://us-cert.cisa.gov/ncas/current-activity/2021/08/25/openssl-releases-security-update

50974556: Overview of F5 vulnerabilities (August 2021)
https://support.f5.com/csp/article/K50974556

Pulse Secure Releases Security Update for Pulse Secure Connect
https://us-cert.cisa.gov/ncas/current-activity/2021/08/06/pulse-secure-releases-security-update-pulse-secure-connect

QNAP works on patches for OpenSSL bugs impacting its NAS devices
https://www.bleepingcomputer.com/news/security/qnap-works-on-patches-for-openssl-bugs-impacting-its-nas-devices/

SAP Releases August 2021 Security Updates
https://us-cert.cisa.gov/ncas/current-activity/2021/08/10/sap-releases-august-2021-security-updates

THE AUGUST 2021 SECURITY UPDATE REVIEW

https://www.zerodayinitiative.com/blog/2021/8/10/the-august-2021-security-update-review

VMware Releases Security Updates for Multiple Products
https://us-cert.cisa.gov/ncas/current-activity/2021/08/05/vmware-releases-security-updates-multiple-products

Windows 10 KB5005033 & KB5005031 cumulative updates released
https://www.bleepingcomputer.com/news/microsoft/windows-10-kb5005033-and-kb5005031-cumulative-updates-released/

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