Some Prevalent CVEs of 2020-2021

Table of Contents

CVE-2021-1675 (PrintNightmare)

CVE-2021-1675 is a remote code execution in Windows Print Spooler. According to the MSRC security bulletin, this vulnerability is reported by Zhipeng Huo, Piotr Madej and Zhang Yunhai. This vulnerability can be used to achieve LPE and RCE. As for the RCE part, you need a user to authenticate on the Spooler service. However, this is still critical in the Domain environment. Because normally DC will have Spooler service enabled, a compromised domain user may use this vulnerability to control the DC.

References:

- https://github.com/calebstewart/CVE-2021-1675
- https://github.com/rapid7/metasploit-framework/pull/15385
- https://github.com/cube0x0/CVE-2021-1675

CVE-2020-0796 (SMBGhost/Coronablue)

A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, aka 'Windows SMBv3 Client/Server Remote Code Execution Vulnerability'.

References:

- https://blog.zecops.com/research/vulnerability-reproduction-cve-2020-0796-poc/
- https://blog.zecops.com/research/smbleedingghost-writeup-chaining-smbleed-cve-2020-1206-with-smbghost/

CVE-2021-26855 (ProxyLogon)

Microsoft Exchange ProxyLogon RCE which allows unauthenticated remote code execution on Microsoft Exchange. Exploitation requires knowledge of the frontend Exchange server URL (e.g., https://exchange.example.org) and an email address for a user on the system. The admin SID and backend can be leaked from the server.

References:

- https://www.rapid7.com/db/modules/exploit/windows/http/exchange_proxylogon_rce/
- https://github.com/praetorian-inc/proxylogon-exploit

CVE-2020-5902

In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages.

References:

- https://github.com/yasserjanah/CVE-2020-5902

CVE-2020-1472 (Zerologon)

CVE-2020-1472 is a privilege escalation vulnerability due to the insecure usage of AES-CFB8 encryption for Netlogon sessions. The AES-CFB8 standard requires that each byte of plaintext, like a password, must have a randomized initialization vector (IV) so that passwords cannot be guessed. The ComputeNetlogonCredential function in Netlogon sets the IV to a fixed 16 bits, which means an attacker could control the deciphered text. An attacker can exploit this flaw to impersonate the identity of any machine on a network when attempting to authenticate to the Domain Controller (DC).

Reference

- https://github.com/SecuraBV/CVE-2020-1472
- https://www.secura.com/blog/zero-logon

CVE-2020-0601 (CurveBall)

A code-level root cause analysis of CVE-2020-0601 in the context of how applications are likely to use CryptoAPI to handle certificates — more specifically in the context of applications communicating via Transport Layer Security (TLS).

References:

- https://www.trendmicro.com/en_us/research/20/b/an-in-depth-technical-analysis-of-curveball-cve-2020-0601.html

CVE-2020-1938 (GhostCat)

CVE-2020-1938 is a file read/inclusion vulnerability in the AJP connector in Apache Tomcat. This is enabled by default with a default configuration port of 8009. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious Java Server Pages (JSP) code within a variety of file types and trigger this vulnerability to gain remote code execution (RCE).

References:

- https://www.chaitin.cn/en/ghostcat

CVE-2020-16898 (Bad Neighbor)

A remote code execution vulnerability exists when the Windows TCP/IP stack improperly handles ICMPv6 Router Advertisement packets that use Option Type 25 (Recursive DNS Server Option) and a length field value that is even.

References:

- https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/bad-neighbors-can-break-windows-cve-2020-16898/

CVE-2020-1350 (aka SIGRed)

This is a critical wormable RCE vulnerability in a Windows DNS Server, which can affect all Windows server versions and can be triggered by a malicious DNS response. Adversaries only need to send a specially generated request to the DNS server to run malicious code in the context of the LocalSystem account (a predefined local account used by the service control manager). The LocalSystem account is not recognized by the security subsystem, and according to Microsoft, the main danger of the vulnerability is that it can be used to spread a threat over a local network.

CVE-2021-1732

It exists in the Windows Win32k operating system kernel and is an elevation-of-privilege (EoP) vulnerability. It would allow a logged-on user to execute code of their choosing with higher privileges, by running a specially crafted application. If successful, attackers could execute code in the context of the kernel and gain SYSTEM privileges, essentially giving the attacker free rein to do whatever they wanted on the compromised machine.

References:

- https://github.com/KaLendsi/CVE-2021-1732-Exploit

CVE-2020-3452

A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct directory traversal attacks and read sensitive files on a targeted system.

References:

- https://github.com/PR3R00T/CVE-2020-3452-Cisco-Scanner

CVE-2021-28480/81

Microsoft Exchange Server Remote Code Execution Vulnerability (pre-authentication). CVE-2021-28480 and CVE-2021-28481 are pre-authentication vulnerabilities in Microsoft Exchange Server. A pre-authentication vulnerability means that an attacker does not need to authenticate to the vulnerable Exchange Server to exploit the vulnerability. All the attacker needs to do is perform reconnaissance against their intended targets and then send specially crafted requests to the vulnerable Exchange Server.

References:

- https://www.tenable.com/blog/cve-2021-28480-cve-2021-28481-cve-2021-28482-cve-2021-28483-four-critical-microsoft-exchange

CVE-2021-28482

Microsoft Exchange Server Remote Code Execution Vulnerability (Post-authentication). Attackers can exploit this deserialization vulnerability if they are authenticated on an on-premises Exchange Server instance.

References:

- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-28482
- https://gist.github.com/testanull/9ebbd6830f7a501e35e67f2fcaa57bda
- https://www.bleepingcomputer.com/news/security/poc-exploit-released-for-microsoft-exchange-bug-discovered-by-nsa/

CVE-2020-16875

A remote code execution vulnerability exists in Microsoft Exchange server due to improper validation of cmdlet arguments. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the System user, aka 'Microsoft Exchange Server Remote Code Execution Vulnerability.

References:

- https://www.rapid7.com/db/vulnerabilities/msft-cve-2020-16875/
- https://packetstormsecurity.com/files/159210/Microsoft-Exchange-Server-DlpUtils-AddTenantDlpPolicy-Remote-Code-Execution.html
- https://srcincite.io/pocs/cve-2020-16875.py.txt
- https://srcincite.io/pocs/cve-2020-16875.ps1.txt

CVE-2020-0688

Microsoft Exchange default MachineKeySection deserialize vulnerability. The CVE-2020-0688 vulnerability affects the Exchange Control Panel (ECP) component. The vulnerability affects all installations of Exchange Server because until the most recent patch, all Exchange Servers had the same validation key and validation algorithm in the web.config file. The POC exploits take advantage of same validation key and validation algorithm to craft a serialized __VIEWSTATE request parameter containing an embedded command, signed with the valid key.

References:

- https://github.com/zcgonvh/CVE-2020-0688
- https://www.exploit-db.com/exploits/48153
- https://www.trustedsec.com/blog/detecting-cve-20200688-remote-code-execution-vulnerability-on-microsoft-exchange-server/

CVE-2020-16952

A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the SharePoint application pool and the SharePoint server farm account. Exploitation of this vulnerability requires that a user uploads a specially crafted SharePoint application package to an affected version of SharePoint.

References:

- https://www.rapid7.com/db/vulnerabilities/msft-cve-2020-16952/

CVE-2021-31956

An EoP vulnerability within Windows NTFS (New Technology File System) which could allow a local user to elevate their privileges on an affected system. A local user could exploit the flaw with a crafted application to take control of a system. This vulnerability affects all currently supported Windows variants including Windows Server and Windows Server Core Installations.

CVE-2021-27070

Windows 10 Update Assistant Elevation of Privilege Vulnerability. The specific flaw exists within the Windows Update Assistant. The issue results from incorrect permissions on a directory. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of Administrator. This vulnerability allows local attackers to escalate privileges on affected installations of Microsoft Windows. An attacker must first obtain the ability to execute low-privileged code on the target system to exploit this vulnerability.

CVE-2021-24090

Windows Error Reporting Elevation of Privilege Vulnerability. The vulnerability exists due to application does not properly impose security restrictions in Windows Error Reporting, which leads to security restrictions bypass and privilege escalation. The vulnerability allows a local attacker to escalate privileges on the system.

CVE-2021-1706

Windows LUAFV Elevation of Privilege Vulnerability. The vulnerability exists due to application does not properly impose security restrictions in Windows LUAFV, which leads to security restrictions bypass and privilege escalation. The vulnerability allows a local user to escalate privileges on the system.

CVE-2021-1701

The vulnerability allows a remote attacker to execute arbitrary code on the system. The vulnerability exists due to insufficient validation of user-supplied input in Remote Procedure Call Runtime. A remote authenticated attacker can pass specially crafted input to the application and execute arbitrary code on the target system.

CVE-2021-1700

The vulnerability allows a remote attacker to execute arbitrary code on the system. The vulnerability exists due to insufficient validation of user-supplied input in Remote Procedure Call Runtime. A

remote authenticated attacker can pass specially crafted input to the application and execute arbitrary code on the target system.

CVE-2021-1668

The vulnerability allows a remote attacker to execute arbitrary code on the system. The vulnerability exists due to insufficient validation of user-supplied input in Microsoft DTV-DVD Video Decoder. A remote attacker can pass specially crafted input to the application and execute arbitrary code on the target system.

CVE-2021-1667

The vulnerability exists due to insufficient validation of user-supplied input in Remote Procedure Call Runtime. A remote authenticated attacker can pass specially crafted input to the application and execute arbitrary code on the target system.

CVE-2020-17096

The vulnerability exists due to insufficient validation of user-supplied input in Windows NTFS. A remote authenticated attacker can pass specially crafted input to the application and execute arbitrary code on the target system.

CVE-2020-17095

The vulnerability exists due to insufficient validation of user-supplied input in Hyper-V. A remote authenticated attacker can pass specially crafted input to the application and execute arbitrary code on the target system.

CVE-2020-17042

The vulnerability exists due to improper input validation in Windows Print Spooler. A remote attacker can send a specially crafted request and execute arbitrary code on the target system. Successful exploitation of this vulnerability may result in complete compromise of the vulnerable system.

CVE-2020-16968

The vulnerability exists due to a boundary error within the Windows Camera Codec Pack. A remote attacker can create a specially crafted file, trick the victim into opening it, trigger memory corruption and execute arbitrary code on the target system. Successful exploitation of this vulnerability may result in complete compromise of the vulnerable system.

CVE-2020-16967

The vulnerability exists due to a boundary error within the Windows Camera Codec Pack. A remote attacker can create a specially crafted file, trick the victim into opening it, trigger memory corruption and execute arbitrary code on the target system.

CVE-2020-16924

The vulnerability exists due to a boundary error within the Windows Jet Database Engine. A remote attacker can create a specially crafted file, trick the victim into opening it, trigger memory corruption and execute arbitrary code on the target system.

CVE-2020-16911

The vulnerability exists due to the way that the Windows Graphics Device Interface Plus (GDI+) handles objects in memory. A local user can use a specially crafted application, trigger out-of-bounds read error and read contents of memory on the system.

CVE-2020-1564

The vulnerability exists due to a boundary error within the Windows Jet Database Engine. A remote attacker can create a specially crafted file, trick the victim into opening it, trigger memory corruption and execute arbitrary code on the target system.

CVE-2020-1562

The vulnerability exists due to a boundary error within Microsoft Graphics Components when processing TTF fonts in fontdrvhost. A remote attacker can create a specially crafted webpage, trick the victim into opening it, trigger use-after-free error and execute arbitrary code on the target system.

CVE-2020-1561

The vulnerability exists due to a boundary error within Microsoft Graphics Components when processing TTF fonts in fontdrvhost. A remote attacker can create a specially crafted webpage, trick the victim into opening it, trigger use-after-free error and execute arbitrary code on the target system.

CVE-2020-1558

The vulnerability exists due to a boundary error within the Windows Jet Database Engine. A remote attacker can create a specially crafted file, trick the victim into opening it, trigger memory corruption and execute arbitrary code on the target system.

CVE-2020-1557

The vulnerability exists due to a boundary error within the Windows Jet Database Engine. A remote attacker can create a specially crafted file, trick the victim into opening it, trigger memory corruption and execute arbitrary code on the target system.

CVE-2020-1508

The vulnerability exists due to a boundary error when Windows Media Audio Decoder improperly handles objects. A remote authenticated attacker can trick a victim to open a specially crafted document or visit a malicious webpage, trigger memory corruption, and execute arbitrary code on the target system.

CVE-2020-1435

The vulnerability exists due to a boundary error when Windows Graphics Device Interface (GDI) handles objects in the memory. A remote attacker can trick a victim to open a specially crafted file or visit a malicious website, trigger memory corruption, and execute arbitrary code on the target system.

CVE-2020-1421

The vulnerability exists due to insufficient validation of user-supplied input in Microsoft Windows. A remote attacker can present to the user a removable drive, or remote share, that contains a malicious .LNK file and execute arbitrary code on the target system.

CVE-2020-1416

The vulnerability exists due to application does not properly impose security restrictions in Visual Studio and Visual Studio Code when they load software dependencies. A local user can plant malicious content on an affected computer and wait for another user to launch Visual Studio or Visual Studio Code, leading to privilege escalation.

CVE-2020-1412

A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Remote Code Execution Vulnerability'.

CVE-2020-1410

A remote code execution vulnerability exists when Windows Address Book (WAB) improperly processes vCard files. To exploit the vulnerability, an attacker could send a malicious vCard that a victim opens using Windows Address Book (WAB), aka 'Windows Address Book Remote Code Execution Vulnerability'.

CVE-2020-1409

A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerability'.

CVE-2020-1408

A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Microsoft Graphics Remote Code Execution Vulnerability'.

CVE-2020-1407

A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1400, CVE-2020-1401.

CVE-2020-1401

A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1400, CVE-2020-1407.

CVE-2020-1400

A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1401, CVE-2020-1407.

CVE-2020-1377

An elevation of privilege vulnerability exists when the Windows Kernel API improperly handles registry objects in memory, aka 'Windows Registry Elevation of Privilege Vulnerability'. An attacker who successfully exploited the vulnerability could gain elevated privileges on a targeted system. A locally authenticated attacker could exploit this vulnerability by running a specially crafted application. The security update addresses the vulnerability by helping to ensure that the Windows Kernel API properly handles objects in memory.

References:

- https://www.rapid7.com/db/vulnerabilities/msft-cve-2020-1377/
- https://github.com/sailay1996/cve-2020-1337-poc

CVE-2020-1319

A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka 'Microsoft Windows Codecs Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1129.

CVE-2020-1317

An elevation of privilege vulnerability exists when Group Policy improperly checks access, aka 'Group Policy Elevation of Privilege Vulnerability'.

CVE-2020-1307

An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1316.

CVE-2020-1299

A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed. An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'.

CVE-2020-1286

A remote code execution vulnerability exists when the Windows Shell does not properly validate file paths. An attacker who successfully exploited this vulnerability could run arbitrary code in the context of the current user, aka 'Windows Shell Remote Code Execution Vulnerability'.

CVE-2020-1285

A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'.

CVE-2020-1248

A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'.

CVE-2020-1236

A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1208.

CVE-2020-1208

A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1236.

CVE-2020-1176

A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1051, CVE-2020-1174, CVE-2020-1175.

CVE-2020-1175

A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1051, CVE-2020-1174, CVE-2020-1176.

CVE-2020-1174

A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1051, CVE-2020-1175, CVE-2020-1176.

CVE-2020-1153

A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Remote Code Execution Vulnerability'.

CVE-2020-1136

A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1028, CVE-2020-1126, CVE-2020-1150.

CVE-2020-1113

A security feature bypass vulnerability exists in Microsoft Windows when the Task Scheduler service fails to properly verify client connections over RPC, aka 'Windows Task Scheduler Security Feature Bypass Vulnerability'.

CVE-2020-1112

An elevation of privilege vulnerability exists when the Windows Background Intelligent Transfer Service (BITS) IIS module improperly handles uploaded content, aka 'Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability'.

CVE-2020-1074

A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1039.

CVE-2020-1067

A remote code execution vulnerability exists in the way that Windows handles objects in memory, aka 'Windows Remote Code Execution Vulnerability'.

CVE-2020-1061

A remote code execution vulnerability exists in the way that the Microsoft Script Runtime handles objects in memory, aka 'Microsoft Script Runtime Remote Code Execution Vulnerability'.

CVE-2020-1054

An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses this vulnerability by correcting how the Windows kernel-mode driver handles objects in memory.

References:

- https://www.cvedetails.com/cve/CVE-2020-1054/
- https://www.rapid7.com/db/vulnerabilities/msft-cve-2020-1054/

.

CVE-2020-1048

An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system. An attacker who successfully exploited this vulnerability could run arbitrary code with elevated system privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted script or application. The update addresses the vulnerability by correcting how the Windows Print Spooler Component writes to the file system.

References:

- https://www.rapid7.com/db/vulnerabilities/msft-cve-2020-1048/
- https://github.com/shubham0d/CVE-2020-1048

CVE-2020-1039

A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1074.

CVE-2020-1013

An elevation of privilege vulnerability exists when Microsoft Windows processes group policy updates, aka 'Group Policy Elevation of Privilege Vulnerability'.

CVE-2020-0997

A remote code execution vulnerability exists when the Windows Camera Codec Pack improperly handles objects in memory, aka 'Windows Camera Codec Pack Remote Code Execution Vulnerability'.

CVE-2021-24094

Microsoft Windows TCP/IP Remote Code Execution Vulnerability.

References:

- https://github.com/0vercl0k/CVE-2021-24086

CVE-2021-24074

This vulnerability exists in the IPv4 source routing which is blocked by default in Windows systems. Attackers, via a crafted IP packet, could exploit this vulnerability to execute arbitrary code on a target host. This vulnerability, with a CVSS score of 9.8, affects all versions of Windows. Affected users are advised to apply the updates for protection as soon as possible.

References:

- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-24074

CVE-2021-1733

A remote code execution vulnerability exists in Windows Remote Desktop Gateway (RD Gateway) when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Gateway (RD Gateway) Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0609.

CVE-2020-0646

A remote code execution vulnerability exists when the Microsoft .NET Framework fails to validate input properly, aka '.NET Framework Remote Code Execution Injection Vulnerability'.

CVE-2020-0668

An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0669, CVE-2020-0670, CVE-2020-0671, CVE-2020-0672.

CVE-2020-0683

An elevation of privilege vulnerability exists in the Windows Installer when MSI packages process symbolic links, aka 'Windows Installer Elevation of Privilege Vulnerability'.

CVE-2020-0787

An elevation of privilege vulnerability exists when the Windows Background Intelligent Transfer Service (BITS) improperly handles symbolic links, aka 'Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability'.

CVE-2020-0796

A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, aka 'Windows SMBv3 Client/Server Remote Code Execution Vulnerability'.

CVE-2020-0863

An information vulnerability exists when Windows Connected User Experiences and Telemetry Service improperly discloses file information, aka 'Connected User Experiences and Telemetry Service Information Disclosure Vulnerability'.

CVE-2020-0932

A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0920, CVE-2020-0929, CVE-2020-0931, CVE-2020-0971, CVE-2020-0974.

CVE-2020-0984

An elevation of privilege vulnerability exists when the Microsoft AutoUpdate (MAU) application for Mac improperly validates updates before executing them, aka 'Microsoft (MAU) Office Elevation of Privilege Vulnerability'.

CVE-2020-1181

A remote code execution vulnerability exists in Microsoft SharePoint Server when it fails to properly identify and filter unsafe ASP.Net web controls, aka 'Microsoft SharePoint Server Remote Code Execution Vulnerability'.

CVE-2020-2551

Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: WLS Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts).

CVE-2020-3452

A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct directory traversal attacks and read sensitive files on a targeted system. The vulnerability is due to a lack of proper input validation of URLs in HTTP requests processed by an affected device. An attacker could exploit this vulnerability by sending a crafted HTTP request containing directory traversal character sequences to an affected device. A successful exploit could allow the attacker to view arbitrary files within the web services file system on the targeted device. The web services file system is enabled when the affected device is configured with either WebVPN or AnyConnect features. This vulnerability cannot be used to obtain access to ASA or FTD system files or underlying operating system (OS) files.

CVE-2020-5902

In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages.

CVE-2020-9484

When using Apache Tomcat versions 10.0.0-M1 to 10.0.0-M4, 9.0.0.M1 to 9.0.34, 8.5.0 to 8.5.54 and 7.0.0 to 7.0.103 if a) an attacker is able to control the contents and name of a file on the server; and b) the server is configured to use the PersistenceManager with a FileStore; and c) the PersistenceManager is configured with sessionAttributeValueClassNameFilter="null" (the default unless a SecurityManager is used) or a sufficiently lax filter to allow the attacker provided object to be deserialized; and d) the attacker knows the relative file path from the storage location used by FileStore to the file the attacker has control over; then, using a specifically crafted request, the attacker will be able to trigger remote code execution via deserialization of the file under their control. Note that all of conditions a) to d) must be true for the attack to succeed.

CVE-2020-14883

Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts).

CVE-2020-14882

Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts).

CVE-2020-14859

Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts).

CVE-2020-13936

An attacker that can modify Velocity templates may execute arbitrary Java code or run arbitrary system commands with the same privileges as the account running the Servlet container. This applies to applications that allow untrusted users to upload/modify velocity templates running Apache Velocity Engine versions up to 2.2.