# Critical Vulnerabilities

## KB5046612: Windows 10 Version 1607 / Windows Server 2016 Security Update (November 2024)

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5046612. It is, therefore, affected by multiple vulnerabilities   - Windows Kerberos Remote Code Execution Vulnerability (CVE-2024-43639)   - Windows NT OS Kernel Elevation of Privilege Vulnerability (CVE-2024-43623)   - Windows Telephony Service Elevation of Privilege Vulnerability (CVE-2024-43626)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Apply Security Update 5046612 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5046612   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.7513 |

## KB5044293: Windows 10 Version 1607 / Windows Server 2016 Security Update (October 2024)

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5044293. It is, therefore, affected by multiple vulnerabilities   - Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability (CVE-2024-38212, CVE-2024-38261, CVE-2024-38265, CVE-2024-43453, CVE-2024-43549, CVE-2024-43564, CVE-2024-43589, CVE-2024-43592, CVE-2024-43593, CVE-2024-43607, CVE-2024-43608, CVE-2024-43611)   - Windows Netlogon Elevation of Privilege Vulnerability (CVE-2024-38124)   - Remote Desktop Client Remote Code Execution Vulnerability (CVE-2024-43599)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Apply Security Update 5044293 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5044293   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.7426 |

## KB5043051: Windows 10 Version 1607 / Windows Server 2016 Security Update (September 2024)

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5043051. It is, therefore, affected by multiple vulnerabilities   - Windows MSHTML Platform Spoofing Vulnerability (CVE-2024-43461)   - Windows Remote Desktop Licensing Service Spoofing Vulnerability (CVE-2024-43455)   - Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability (CVE-2024-38260, CVE-2024-38263, CVE-2024-43454, CVE-2024-43467)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Apply Security Update 5043051 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5043051   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.7330 |

## KB5041773: Windows 10 Version 1607 / Windows Server 2016 Security Update (August 2024)

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5041773. It is, therefore, affected by multiple vulnerabilities   - An elevation of privilege vulnerability exists in Windows based systems supporting Virtualization Based Security (VBS) including a subset of Azure Virtual Machine SKUS. This can allow an attacker with administrator privileges to replace current versions of Windows system files with outdated versions. By exploiting this vulnerability, an attacker could reintroduce previously mitigated vulnerabilities, circumvent some features of VBS, and exfiltrate data protected by VBS. (CVE-2024-21302)   - A buffer overflow was found in grub\_font\_construct\_glyph(). A malicious crafted pf2 font can lead to an overflow when calculating the max\_glyph\_size value, allocating a smaller than needed buffer for the glyph, this further leads to a buffer overflow and a heap based out-of-bounds write. An attacker may use this vulnerability to circumvent the secure boot mechanism. (CVE-2022-2601)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Apply Security Update 5041773 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5041773   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.7254 |

## KB5040434: Windows 10 Version 1607 / Windows Server 2016 Security Update (July 2024)

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5040434. It is, therefore, affected by multiple vulnerabilities   - RADIUS Protocol under RFC 2865 is susceptible to forgery attacks by a local attacker who can modify any valid Response (Access-Accept, Access-Reject, or Access-Challenge) to any other response using a chosen- prefix collision attack against MD5 Response Authenticator signature. (CVE-2024-3596)   - A remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands. (CVE-2024-30013, CVE-2024-38104) Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Apply Security Update 5040434 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5040434   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.7155 |

## KB5039214: Windows 10 Version 1607 / Windows Server 2016 Security Update (June 2024)

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5039214. It is, therefore, affected by multiple vulnerabilities   - Microsoft Speech Application Programming Interface (SAPI) Remote Code Execution Vulnerability (CVE-2024-30097)   - Windows Remote Access Connection Manager Information Disclosure Vulnerability (CVE-2024-30069)   - DHCP Server Service Denial of Service Vulnerability (CVE-2024-30070)   - Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability (CVE-2024-30080)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Apply Security Update 5039214 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5039214   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.7070 |

## KB5032197: Windows 10 Version 1607 and Windows Server 2016 Security Update (November 2023)

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5032197. It is, therefore, affected by multiple vulnerabilities   - Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability (CVE-2023-36402)   - Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability (CVE-2023-36397)   - Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability (CVE-2023-36028)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Apply Security Update 5032197 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5032197   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.6451 |

## KB5031362: Windows 10 Version 1607 and Windows Server 2016 Security Update (October 2023)

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5031362. It is, therefore, affected by multiple vulnerabilities   - The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023. (CVE-2023-44487)   - Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability (CVE-2023-36577)   - Windows IIS Server Elevation of Privilege Vulnerability (CVE-2023-36434)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Apply Security Update 5031362 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5031362   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.6343 |

## KB5029242: Windows 10 Version 1607 and Windows Server 2016 Security Update (August 2023)

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5029242. It is, therefore, affected by multiple vulnerabilities   - Microsoft Message Queuing Remote Code Execution Vulnerability (CVE-2023-35385, CVE-2023-36910, CVE-2023-36911)   - Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability (CVE-2023-36882)   - Windows Bluetooth A2DP driver Elevation of Privilege Vulnerability (CVE-2023-35387)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Apply Security Update 5029242 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5029242   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.6167 |

## KB5028169: Windows 10 Version 1607 and Windows Server 2016 Security Update (July 2023)

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5028169. It is, therefore, affected by multiple vulnerabilities   - Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability (CVE-2023-35365, CVE-2023-35366, CVE-2023-35367)   - Windows Netlogon Information Disclosure Vulnerability (CVE-2023-21526)   - Windows Win32k Elevation of Privilege Vulnerability (CVE-2023-21756)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Apply Security Update 5028169 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5028169   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.6085 |

## KB5027219: Windows 10 Version 1607 and Windows Server 2016 Security Update (June 2023)

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5027219. It is, therefore, affected by multiple vulnerabilities   - Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability (CVE-2023-29363, CVE-2023-32014, CVE-2023-32015)   - Windows Collaborative Translation Framework Elevation of Privilege Vulnerability (CVE-2023-32009)   - Microsoft ODBC Driver Remote Code Execution Vulnerability (CVE-2023-29373)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Apply Security Update 5027219 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5027219   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.5989 |

## KB5026363: Windows 10 Version 1607 and Windows Server 2016 Security Update (May 2023)

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5026363. It is, therefore, affected by multiple vulnerabilities   - Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability (CVE-2023-24943)   - Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability (CVE-2023-28283)   - Server for NFS Denial of Service Vulnerability (CVE-2023-24939)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Apply Security Update 5026363 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5026363   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.5921 |

## KB5025228: Windows 10 Version 1607 and Windows Server 2016 Security Update (April 2023)

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5025228. It is, therefore, affected by multiple vulnerabilities   - Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability (CVE-2023-28275)   - Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability (CVE-2023-28250)   - Microsoft Message Queuing Remote Code Execution Vulnerability (CVE-2023-21554)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Apply Security Update 5025228 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5025228   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.5850 |

## KB5023697: Windows 10 Version 1607 and Windows Server 2016 Security Update (March 2023)

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5023697. It is, therefore, affected by multiple vulnerabilities   - An out-of-bounds write vulnerability exists in TPM2.0's Module Library allowing writing of a 2-byte data past the end of TPM2.0 command in the CryptParameterDecryption routine. An attacker who can successfully exploit this vulnerability can lead to denial of service (crashing the TPM chip/process or rendering it unusable) and/or arbitrary code execution in the TPM context. (CVE-2023-1017)   - An out-of-bounds read vulnerability exists in TPM2.0's Module Library allowing a 2-byte read past the end of a TPM2.0 command in the CryptParameterDecryption routine. An attacker who can successfully exploit this vulnerability can read or access sensitive data stored in the TPM. (CVE-2023-1018)   - Remote Procedure Call Runtime Remote Code Execution Vulnerability (CVE-2023-21708, CVE-2023-23405, CVE-2023-24869, CVE-2023-24908)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Apply Security Update 5023697 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5023697   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.5786 |

## KB5022838: Windows 10 Version 1607 and Windows Server 2016 Security Update (February 2023)

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5022838. It is, therefore, affected by multiple vulnerabilities   - Windows iSCSI Discovery Service Remote Code Execution Vulnerability (CVE-2023-21803)   - Microsoft PostScript Printer Driver Remote Code Execution Vulnerability (CVE-2023-21684, CVE-2023-21801)   - Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability (CVE-2023-21685, CVE-2023-21686, CVE-2023-21799)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Apply Security Update 5022838 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5022838   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.5717 |

## KB5017305: Windows 10 Version 1607 and Windows Server 2016 Security Update (September 2022)

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5017305. It is, therefore, affected by multiple vulnerabilities   - Windows Photo Import API Elevation of Privilege Vulnerability (CVE-2022-26928)   - Windows Credential Roaming Service Elevation of Privilege Vulnerability (CVE-2022-30170)   - Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability (CVE-2022-30200)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Apply Security Update 5017305 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5017305   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.5356 |

## KB5016622: Windows 10 Version 1607 and Windows Server 2016 Security Update (August 2022)

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5016622. It is, therefore, affected by multiple vulnerabilities   - Windows Point-to-Point Protocol (PPP) Denial of Service Vulnerability (CVE-2022-35747, CVE-2022-35769)   - Windows Point-to-Point Protocol (PPP) Remote Code Execution Vulnerability (CVE-2022-30133, CVE-2022-35744)   - Windows Bluetooth Service Remote Code Execution Vulnerability (CVE-2022-30144)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Apply Security Update 5016622 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5016622   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.5291 |

## KB5014702: Windows 10 Version 1607 and Windows Server 2016 Security Update (June 2022)

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5014702. It is, therefore, affected by multiple vulnerabilities   - Windows Network File System Remote Code Execution Vulnerability (CVE-2022-30136)   - Windows Kerberos Elevation of Privilege Vulnerability (CVE-2022-30165)   - Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability (CVE-2022-30139, CVE-2022-30141, CVE-2022-30143, CVE-2022-30146, CVE-2022-30149, CVE-2022-30153, CVE-2022-30161)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Apply Security Update 5014702 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5014702   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.5192 |

## KB5012596: Windows 10 version 1607 / Windows Server 2016 Security Update (April 2022)

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5012591. It is, therefore, affected by multiple vulnerabilities:   - An elevation of privilege vulnerability. An attacker can exploit this to gain elevated privileges.  (CVE-2022-26827, CVE-2022-24549, CVE-2022-26810, CVE-2022-26803, CVE-2022-26808, CVE-2022-26807, CVE-2022-26792, CVE-2022-26801, CVE-2022-26802, CVE-2022-26794, CVE-2022-26790, CVE-2022-26797, CVE-2022-26787, CVE-2022-26798, CVE-2022-26796, CVE-2022-26786, CVE-2022-26904, CVE-2022-26788, CVE-2022-24496, CVE-2022-24544, CVE-2022-24540, CVE-2022-24489, CVE-2022-24486, CVE-2022-24481, CVE-2022-24479, CVE-2022-24527, CVE-2022-24474, CVE-2022-24521, CVE-2022-24547, CVE-2022-24550, CVE-2022-24499, CVE-2022-24494, CVE-2022-24542, CVE-2022-24530)   - A denial of service (DoS) vulnerability. An attacker can exploit this issue to cause the affected component to deny system or application services. (CVE-2022-26831, CVE-2022-26915, CVE-2022-24538, CVE-2022-24484, CVE-2022-26784)   - A remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands. (CVE-2022-26823, CVE-2022-26812, CVE-2022-26919, CVE-2022-26811, CVE-2022-26809, CVE-2022-26918, CVE-2022-26917, CVE-2022-26813, CVE-2022-26826, CVE-2022-26824, CVE-2022-26815, CVE-2022-26814, CVE-2022-26916, CVE-2022-26822, CVE-2022-26829, CVE-2022-26820, CVE-2022-26819, CVE-2022-26818, CVE-2022-26825, CVE-2022-26817, CVE-2022-26821, CVE-2022-24545, CVE-2022-24541, CVE-2022-24492, CVE-2022-24491, CVE-2022-24537, CVE-2022-24536, CVE-2022-24487, CVE-2022-24534, CVE-2022-24485, CVE-2022-24533, CVE-2022-26903, CVE-2022-24495, CVE-2022-24528, CVE-2022-21983, CVE-2022-22008, CVE-2022-24500)   - An information disclosure vulnerability. An attacker can exploit this to disclose potentially sensitive information. (CVE-2022-26816, CVE-2022-24493, CVE-2022-24539, CVE-2022-24490, CVE-2022-26783, CVE-2022-26785, CVE-2022-24498, CVE-2022-24483) |
| Recommendation | Apply Cumulative Update 5012596 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5012596   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.5066 |

## KB5009546: Windows 10 Version 1607 and Windows Server 2016 Security Update (January 2022)

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5009546. It is, therefore, affected by multiple vulnerabilities:   - A remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands. (CVE-2022-21849, CVE-2022-21850, CVE-2022-21851, CVE-2022-21874, CVE-2022-21878, CVE-2022-21892, CVE-2022-21893, CVE-2022-21922, CVE-2022-21928, CVE-2022-21958, CVE-2022-21959, CVE-2022-21960, CVE-2022-21961, CVE-2022-21962, CVE-2022-21963)   - An information disclosure vulnerability. An attacker can exploit this to disclose potentially sensitive information. (CVE-2022-21876, CVE-2022-21880, CVE-2022-21904, CVE-2022-21915)   - A security feature bypass vulnerability exists. An attacker can exploit this and bypass the security feature and perform unauthorized actions compromising the integrity of the system/application.  (CVE-2022-21894, CVE-2022-21900, CVE-2022-21905, CVE-2022-21913, CVE-2022-21924, CVE-2022-21925)   - A session spoofing vulnerability exists. An attacker can exploit this to perform actions with the privileges of another user. (CVE-2022-21836)   - A denial of service (DoS) vulnerability. An attacker can exploit this issue to cause the affected component to deny system or application services. (CVE-2022-21843, CVE-2022-21848, CVE-2022-21883, CVE-2022-21889, CVE-2022-21890)   - An elevation of privilege vulnerability. An attacker can exploit this to gain elevated privileges.  (CVE-2022-21833, CVE-2022-21834, CVE-2022-21835, CVE-2022-21838, CVE-2022-21857, CVE-2022-21859, CVE-2022-21860, CVE-2022-21862, CVE-2022-21863, CVE-2022-21864, CVE-2022-21866, CVE-2022-21867, CVE-2022-21868, CVE-2022-21870, CVE-2022-21871, CVE-2022-21873, CVE-2022-21875, CVE-2022-21879, CVE-2022-21881, CVE-2022-21884, CVE-2022-21885, CVE-2022-21895, CVE-2022-21897, CVE-2022-21901, CVE-2022-21902, CVE-2022-21903, CVE-2022-21908, CVE-2022-21910, CVE-2022-21914, CVE-2022-21916, CVE-2022-21919, CVE-2022-21920) |
| Recommendation | Apply Cumulative Update KB5009546. |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5009546   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.4886 |

## KB5008207: Windows 10 Version 1607 and Windows Server 2016 Security Update (December 2021)

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5008207. It is, therefore, affected by multiple vulnerabilities:   - A remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands. (CVE-2021-43215, CVE-2021-43217, CVE-2021-43232, CVE-2021-43233, CVE-2021-43234)   - An information disclosure vulnerability. An attacker can exploit this to disclose potentially sensitive information. (CVE-2021-43216, CVE-2021-43222, CVE-2021-43224, CVE-2021-43227, CVE-2021-43235, CVE-2021-43236)   - An elevation of privilege vulnerability. An attacker can exploit this to gain elevated privileges.  (CVE-2021-41333, CVE-2021-43207, CVE-2021-43223, CVE-2021-43226, CVE-2021-43229, CVE-2021-43230, CVE-2021-43231, CVE-2021-43238, CVE-2021-43248, CVE-2021-43883, CVE-2021-43893) |
| Recommendation | Apply Cumulative Update KB5008207. |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5008207   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.4825 |

## KB5005043: Windows 10 Version 1607 and Windows Server 2016 Security Update (August 2021)

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5005043. It is, therefore, affected by multiple vulnerabilities :   - A remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands. (CVE-2021-26424, CVE-2021-26432, CVE-2021-34530, CVE-2021-34533, CVE-2021-34534, CVE-2021-34535, CVE-2021-36936, CVE-2021-36937, CVE-2021-36947)   - A session spoofing vulnerability exists. An attacker can exploit this to perform actions with the privileges of another user. (CVE-2021-36942)   - An elevation of privilege vulnerability. An attacker can exploit this to gain elevated privileges.  (CVE-2021-26425, CVE-2021-26426, CVE-2021-34483, CVE-2021-34484, CVE-2021-34487, CVE-2021-34536, CVE-2021-34537)   - An memory corruption vulnerability exists. An attacker can exploit this to corrupt the memory and cause unexpected behaviors within the system/application.  (CVE-2021-34480)   - An information disclosure vulnerability. An attacker can exploit this to disclose potentially sensitive information. (CVE-2021-26433, CVE-2021-36926, CVE-2021-36932, CVE-2021-36933, CVE-2021-36938) |
| Recommendation | Apply Cumulative Update KB5005043. |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5005043   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.4583 |

## KB5004238: Windows 10 Version 1607 / Windows Server 2016 Security Update (July 2021)

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5004238. It is, therefore, affected by multiple vulnerabilities. |
| Recommendation | Apply Cumulative Update 5004238 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5004238   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.4530 |

## KB5003638: Windows 10 version 1607 / Windows Server 2016 Security Update (June 2021)

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5003638. It is, therefore, affected by multiple vulnerabilities |
| Recommendation | Apply Cumulative Update 5003638 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5003638   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.4467 |

## Microsoft .NET Core SEoL

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | An unsupported version of Microsoft .NET Core is installed on the remote host. |
| Description | According to its version, the Microsoft .NET Core installed on the remote host is no longer maintained by its vendor or provider.  Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities. |
| Recommendation | Upgrade to a version of Microsoft .NET Core that is currently supported. |
| Evidence | Path : C:\Program Files\dotnet\shared\Microsoft.NetCore.App\3.1.16\  Installed version : 3.1.16.30112  Security End of Life : December 13, 2022  Time since Security End of Life (Est.) : >= 1 year |

## Microsoft .NET Core SEoL

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | An unsupported version of Microsoft .NET Core is installed on the remote host. |
| Description | According to its version, the Microsoft .NET Core installed on the remote host is no longer maintained by its vendor or provider.  Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities. |
| Recommendation | Upgrade to a version of Microsoft .NET Core that is currently supported. |
| Evidence | Path : C:\Program Files\dotnet\shared\Microsoft.NetCore.App\6.0.25\  Installed version : 6.0.25.33020  Security End of Life : November 12, 2024  Time since Security End of Life (Est.) : >= 1 week |

## ASP.NET Core SEoL

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | An unsupported version of ASP.NET Core is installed on the remote host. |
| Description | According to its version, the ASP.NET Core installed on the remote host is no longer maintained by its vendor or provider.  Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities. |
| Recommendation | Upgrade to a version of ASP.NET Core that is currently supported. |
| Evidence | Path : C:\Program Files\dotnet\shared\Microsoft.AspNetCore.App\3.1.16  Installed version : 3.1.16  Security End of Life : December 13, 2022  Time since Security End of Life (Est.) : >= 1 year |

## ASP.NET Core SEoL

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | An unsupported version of ASP.NET Core is installed on the remote host. |
| Description | According to its version, the ASP.NET Core installed on the remote host is no longer maintained by its vendor or provider.  Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities. |
| Recommendation | Upgrade to a version of ASP.NET Core that is currently supported. |
| Evidence | Path : C:\Program Files\dotnet\shared\Microsoft.AspNetCore.App\6.0.25  Installed version : 6.0.25  Security End of Life : November 12, 2024  Time since Security End of Life (Est.) : >= 1 week |

## Microsoft SQL Server Unsupported Version Detection (remote check)

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | An unsupported version of a database server is running on the remote host. |
| Description | According to its self-reported version number, the installation of Microsoft SQL Server on the remote host is no longer supported.  Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. |
| Recommendation | Upgrade to a version of Microsoft SQL Server that is currently supported. |
| Evidence | The following unsupported installation of Microsoft SQL Server was detected :    Installed version : 13.0.5026.0  Fixed version : 13.0.6300.2 (2016 SP3)   SQL Server Instance : VEEAMSQL2016 |

## Microsoft SQL Server Unsupported Version Detection

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | An unsupported version of a database server is running on the remote host. |
| Description | According to its self-reported version number, the installation of Microsoft SQL Server on the remote host is no longer supported.  Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. |
| Recommendation | Upgrade to a version of Microsoft SQL Server that is currently supported. |
| Evidence | The following unsupported installations of Microsoft SQL Server were detected :   Installed version : 13.0.5026.0 Express Edition  Install path : C:\Program Files\Microsoft SQL Server\MSSQL13.VEEAMSQL2016\MSSQL\Binn  Instance : VEEAMSQL2016  Minimum supported version : 13.0.6300.2 (2016 SP3) |

## Veeam Backup and Replication 12.x < 12.2.0.334 Multiple Vulnerabilities (September 2024) (KB4649)

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | The version of Veeam Backup and Replication installed on the remote Windows host is affected by multiple vulnerabilities. |
| Description | The version of Veeam Backup and Replication installed on the remote Windows host is 12.x prior to 12.2.0.334. It is, therefore, affected by multiple vulnerabilities, including:   - A vulnerability allowing unauthenticated remote code execution (RCE). (CVE-2024-40711)   - A vulnerability that allows a user who has been assigned a low-privileged role within Veeam Backup & Replication to alter Multi-Factor Authentication (MFA) settings and bypass MFA. (CVE-2024-40713)   - A series of related high-severity vulnerabilities, the most notable enabling remote code execution (RCE) as the service account and extraction of sensitive information (saved credentials and passwords). (CVE-2024-40710)  Note that Nessus has not tested for this issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to Veeam Backup and Replication version 12.2.0.334 or later. |
| Evidence | Path : C:\Program Files\Veeam\Backup and Replication\Backup\  Installed version : 12.1.1.56  Fixed version : 12.2.0.334 |

## Google Chrome < 128.0.6613.84 Multiple Vulnerabilities

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | A web browser installed on the remote Windows host is affected by multiple vulnerabilities. |
| Description | The version of Google Chrome installed on the remote Windows host is prior to 128.0.6613.84. It is, therefore, affected by multiple vulnerabilities as referenced in the 2024\_08\_stable-channel-update-for-desktop\_21 advisory.   - Use after free in Passwords in Google Chrome on Android prior to 128.0.6613.84 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-7964)   - Inappropriate implementation in V8 in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-7965)   - Out of bounds memory access in Skia in Google Chrome prior to 128.0.6613.84 allowed a remote attacker who had compromised the renderer process to perform out of bounds memory access via a crafted HTML page.  (Chromium security severity: High) (CVE-2024-7966)   - Heap buffer overflow in Fonts in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-7967)   - Use after free in Autofill in Google Chrome prior to 128.0.6613.84 allowed a remote attacker who had convinced the user to engage in specific UI interactions to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-7968)   - Type confusion in V8 in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-7971)   - Inappropriate implementation in V8 in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity:  Medium) (CVE-2024-7972)   - Heap buffer overflow in PDFium in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file. (Chromium security severity: Medium) (CVE-2024-7973)   - Insufficient data validation in V8 API in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to potentially exploit heap corruption via a crafted Chrome Extension. (Chromium security severity:  Medium) (CVE-2024-7974)   - Inappropriate implementation in Permissions in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium) (CVE-2024-7975)   - Inappropriate implementation in FedCM in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium) (CVE-2024-7976)   - Insufficient data validation in Installer in Google Chrome on Windows prior to 128.0.6613.84 allowed a local attacker to perform privilege escalation via a malicious file. (Chromium security severity: Medium) (CVE-2024-7977)   - Insufficient policy enforcement in Data Transfer in Google Chrome prior to 128.0.6613.84 allowed a remote attacker who convinced a user to engage in specific UI gestures to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium) (CVE-2024-7978)   - Insufficient data validation in Installer in Google Chrome on Windows prior to 128.0.6613.84 allowed a local attacker to perform privilege escalation via a crafted symbolic link. (Chromium security severity:  Medium) (CVE-2024-7979, CVE-2024-7980)   - Inappropriate implementation in Views in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low) (CVE-2024-7981)   - Inappropriate implementation in WebApp Installs in Google Chrome on Windows prior to 128.0.6613.84 allowed an attacker who convinced a user to install a malicious application to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low) (CVE-2024-8033)   - Inappropriate implementation in Custom Tabs in Google Chrome on Android prior to 128.0.6613.84 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low) (CVE-2024-8034)   - Inappropriate implementation in Extensions in Google Chrome on Windows prior to 128.0.6613.84 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low) (CVE-2024-8035)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to Google Chrome version 128.0.6613.84 or later. |
| Evidence | Path : C:\Program Files\Google\Chrome\Application  Installed version : 126.0.6478.128  Fixed version : 128.0.6613.84 |

## Veeam Backup and Replication with Veeam Backup Enterprise Manager Multiple Vulnerabilities (KB4581)

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | The version of Veeam Backup and Replication with Veeam Backup Enterprise Manager installed on the remote Windows host is affected by multiple vulnerabilities. |
| Description | The version of Veeam Backup and Replication with Veeam Backup Enterprise Manager installed on the remote Windows host is prior to 12.1.2.172. It is, therefore, affected by multiple vulnerabilities:   - A vulnerability in Veeam Backup Enterprise Manager that allows an unauthenticated attacker to log in to the Veeam Backup Enterprise Manager web interface as any user. (CVE-2024-29849)   - A vulnerability in Veeam Backup Enterprise Manager that allows account takeover via NTLM relay. (CVE-2024-29850)   - A vulnerability in Veeam Backup Enterprise Manager that allows a high-privileged user to steal the NTLM hash of the Veeam Backup Enterprise Manager service account if that service account is anything other than the default Local System account. (CVE-2024-29851)   - A vulnerability in Veeam Backup Enterprise Manager that allows high-privileged users to read backup session logs.  (CVE-2024-29852)  Note that Nessus has not tested for this issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to Veeam Backup and Replication version 12.1.2.172 or later. |
| Evidence | Path : C:\Program Files\Veeam\Backup and Replication\Backup\  Installed version : 12.1.1.56  Fixed version : 12.1.2.172 |

## Security Update for Microsoft .NET Core (January 2024)

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | The remote Windows host is affected by a .NET Core vulnerability |
| Description | The version of tested product installed on the remote host is prior to tested version. It is, therefore, affected by multiple vulnerabilities as referenced in the 2024\_Jan\_09 advisory.   - NET, .NET Framework, and Visual Studio Security Feature Bypass Vulnerability (CVE-2024-0057)   - .NET Denial of Service Vulnerability (CVE-2024-20672)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Update .NET Core, remove vulnerable packages and refer to vendor advisory. |
| Evidence | Path : C:\Program Files\dotnet\shared\Microsoft.NetCore.App\6.0.25\  Installed version : 6.0.25.33020  Fixed version : 6.0.26 |

## WinSCP < 5.17.10 RCE

|  |  |
| --- | --- |
| Criticality | Critical |
| Synopsis | A file transfer application installed on the remote Windows host is affected by a remote code execution vulnerability. |
| Description | The version of WinSCP installed on the remote Windows host is prior to 5.17.10. It is, therefore, affected by a remote code execution vulnerability that allows remote attackers to execute arbitrary programs when the URL handler encounters a crafted URL that loads session settings. (For example, this is exploitable in a default installation in which WinSCP is the handler for sftp:// URLs.)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to WinSCP version 5.17.10 or later. |
| Evidence | Path : C:\Program Files (x86)\WinSCP\  Installed version : 5.15.1.9407  Fixed version : 5.17.10 |

# High Vulnerabilities

## KB5037763: Windows 10 Version 1607 / Windows Server 2016 Security Update (May 2024)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5037763. It is, therefore, affected by multiple vulnerabilities   - Windows MSHTML Platform Security Feature Bypass Vulnerability (CVE-2024-30040)   - Windows Common Log File System Driver Elevation of Privilege Vulnerability (CVE-2024-29996, CVE-2024-30025, CVE-2024-30037)   - Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability (CVE-2024-30006)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Apply Security Update 5037763 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5037763   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.6981 |

## KB5036899: Windows 10 Version 1607 / Windows Server 2016 Security Update (April 2024)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5036899. It is, therefore, affected by multiple vulnerabilities   - Microsoft WDAC SQL Server ODBC Driver Remote Code Execution Vulnerability (CVE-2024-26214)   - Secure Boot Security Feature Bypass Vulnerability (CVE-2024-20669, CVE-2024-26168, CVE-2024-26171, CVE-2024-26175, CVE-2024-26180, CVE-2024-26189, CVE-2024-26194, CVE-2024-26240, CVE-2024-26250, CVE-2024-28896, CVE-2024-28897, CVE-2024-28898, CVE-2024-28903, CVE-2024-28919, CVE-2024-28921, CVE-2024-28922, CVE-2024-28923, CVE-2024-28924, CVE-2024-28925, CVE-2024-29061, CVE-2024-29062)   - Windows rndismp6.sys Remote Code Execution Vulnerability (CVE-2024-26252, CVE-2024-26253)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Apply Security Update 5036899 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5036899   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.6897 |

## KB5035855: Windows 10 Version 1607 / Windows Server 2016 Security Update (March 2024)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5035855. It is, therefore, affected by multiple vulnerabilities   - Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability (CVE-2024-21441, CVE-2024-21444, CVE-2024-21450, CVE-2024-26161, CVE-2024-26166)   - Windows USB Hub Driver Remote Code Execution Vulnerability (CVE-2024-21429)   - Windows USB Attached SCSI (UAS) Protocol Remote Code Execution Vulnerability (CVE-2024-21430)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Apply Security Update 5035855 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5035855   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.6795 |

## Security Update for Microsoft ASP.NET Core (February 2024) (CVE-2024-21386)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The remote Windows host is affected by a ASP.NET Core vulnerability |
| Description | The version of tested product installed on the remote host is prior to tested version. It is, therefore, affected by a denial of service as referenced in the vendor advisory.    - ASP.NET Core Denial of Service Vulnerability  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Update .NET Core, remove vulnerable packages and refer to vendor advisory. |
| Evidence | Path : C:\Program Files\dotnet\shared\Microsoft.AspNetCore.App\6.0.25  Installed version : 6.0.25  Fixed version : 6.0.27 |

## KB5034767: Windows 10 Version 1607 and Windows Server 2016 Security Update (February 2024)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5034767. It is, therefore, affected by multiple vulnerabilities   - Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability (CVE-2024-21350, CVE-2024-21352, CVE-2024-21358, CVE-2024-21359, CVE-2024-21360, CVE-2024-21361, CVE-2024-21365, CVE-2024-21366, CVE-2024-21367, CVE-2024-21368, CVE-2024-21369, CVE-2024-21370, CVE-2024-21375, CVE-2024-21391, CVE-2024-21420)   - Windows Kernel Information Disclosure Vulnerability (CVE-2024-21340)   - Microsoft ActiveX Data Objects Remote Code Execution Vulnerability (CVE-2024-21349)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Apply Security Update 5034767 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5034767   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.6707 |

## KB5034119: Windows 10 Version 1607 and Windows Server 2016 Security Update (January 2024)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5034119. It is, therefore, affected by multiple vulnerabilities   - Microsoft ODBC Driver Remote Code Execution Vulnerability (CVE-2024-20654)   - BitLocker Security Feature Bypass Vulnerability (CVE-2024-20666)   - Windows Kerberos Security Feature Bypass Vulnerability (CVE-2024-20674)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Apply Security Update 5034119 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5034119   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.6611 |

## KB5033373: Windows 10 Version 1607 and Windows Server 2016 Security Update (December 2023)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5033373. It is, therefore, affected by multiple vulnerabilities   - Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability (CVE-2023-36006)   - Win32k Elevation of Privilege Vulnerability (CVE-2023-36011)   - A division-by-zero error on some AMD processors can potentially return speculative data resulting in loss of confidentiality. (CVE-2023-20588)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Apply Security Update 5033373 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5033373   - C:\Windows\system32\pcadm.dll has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.6529 |

## KB5030213: Windows 10 Version 1607 and Windows Server 2016 Security Update (September 2023)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5030213. It is, therefore, affected by multiple vulnerabilities   - DHCP Server Service Denial of Service Vulnerability (CVE-2023-38162)   - Windows GDI Elevation of Privilege Vulnerability (CVE-2023-36804, CVE-2023-38161)   - DHCP Server Service Information Disclosure Vulnerability (CVE-2023-36801, CVE-2023-38152)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Apply Security Update 5030213 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5030213   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.6252 |

## KB5022289: Windows 10 Version 1607 and Windows Server 2016 Security Update (January 2023)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5022289. It is, therefore, affected by multiple vulnerabilities   - Microsoft ODBC Driver Remote Code Execution Vulnerability (CVE-2023-21732)   - Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability (CVE-2023-21681)   - Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability (CVE-2023-21674)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Apply Security Update 5022289 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5022289   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.5648 |

## Security Updates for Microsoft ASP.NET Core (December 2022)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The Microsoft ASP.NET core installations on the remote host are affected by remote code execution vulnerability. |
| Description | A remote code execution vulnerability exists in ASP.NET core 3.1, ASP.NET 6.0, and ASP.NET 7.0, where a malicious actor could cause a user to run arbitrary code as a result of parsing maliciously crafted xps files.  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. |
| Recommendation | Update ASP.NET Core Runtime to version 3.1.32 or 6.0.12 or 7.0.1. |
| Evidence | Path : C:\Program Files\dotnet\shared\Microsoft.AspNetCore.App\3.1.16  Installed version : 3.1.16  Fixed version : 3.1.32 |

## KB5021235: Windows 10 Version 1607 and Windows Server 2016 Security Update (December 2022)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5021235. It is, therefore, affected by multiple vulnerabilities   - PowerShell Remote Code Execution Vulnerability (CVE-2022-41076)   - A remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands. (CVE-2022-44670, CVE-2022-44676)   Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Apply Security Update 5021235 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5021235   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.5582 |

## KB5019964: Windows 10 Version 1607 and Windows Server 2016 Security Update (November 2022)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5019964. It is, therefore, affected by multiple vulnerabilities   - AMD: CVE-2022-23824 IBPB and Return Address Predictor Interactions (CVE-2022-23824)   - Windows Kerberos RC4-HMAC Elevation of Privilege Vulnerability (CVE-2022-37966)   - Windows Kerberos Elevation of Privilege Vulnerability (CVE-2022-37967)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Apply Security Update 5019964 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5019964   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.5501 |

## WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The remote Windows host is potentially missing a mitigation for a remote code execution vulnerability. |
| Description | The remote system may be in a vulnerable state to CVE-2013-3900 due to a missing or misconfigured registry keys:  - HKEY\_LOCAL\_MACHINE\Software\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck  - HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck An unauthenticated, remote attacker could exploit this, by sending specially crafted requests, to execute arbitrary code on an affected host. |
| Recommendation | Add and enable registry value EnableCertPaddingCheck:  - HKEY\_LOCAL\_MACHINE\Software\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck  Additionally, on 64 Bit OS systems, Add and enable registry value EnableCertPaddingCheck:   - HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck |
| Evidence | Nessus detected the following potentially insecure registry key configuration:  - Software\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck is not present in the registry.  - Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck is not present in the registry. |

## KB5018411: Windows 10 Version 1607 and Windows Server 2016 Security Update (October 2022)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5018411. It is, therefore, affected by multiple vulnerabilities   - Server Service Remote Protocol Elevation of Privilege Vulnerability (CVE-2022-38045)   - Microsoft ODBC Driver Remote Code Execution Vulnerability (CVE-2022-38040)   - Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability (CVE-2022-37982, CVE-2022-38031)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Apply Security Update 5018411 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5018411   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.5427 |

## Security Updates for Microsoft ASP.NET Core (September 2022)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The Microsoft ASP.NET Core installations on the remote host are missing a security update. |
| Description | A denial of service vulnerability exists in ASP.NET core 6.0 < 6.0.9 and ASP.NET Core 3.1 < 3.1.29. An unauthenticated, remote attacker can exploit this, by sending a customized payload that is parsed during model binding, to cause a stack overflow, which may cause the application to stop responding.  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. |
| Recommendation | Update ASP.NET Core Runtime to version 3.1.29 or 6.0.9. |
| Evidence | Path : C:\Program Files\dotnet\shared\Microsoft.AspNetCore.App\3.1.16  Installed version : 3.1.16  Fixed version : 3.1.29 |

## KB5015808: Windows 10 Version 1607 and Windows Server 2016 Security Update (July 2022)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5015808. It is, therefore, affected by multiple vulnerabilities:   - A remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands. (CVE-2022-22024, CVE-2022-22027, CVE-2022-22029, CVE-2022-22038, CVE-2022-22039, CVE-2022-30211, CVE-2022-30214, CVE-2022-30221, CVE-2022-30222)   - A security feature bypass vulnerability exists. An attacker can exploit this and bypass the security feature and perform unauthorized actions compromising the integrity of the system/application.  (CVE-2022-22023, CVE-2022-22048, CVE-2022-30203)   - A denial of service (DoS) vulnerability. An attacker can exploit this issue to cause the affected component to deny system or application services. (CVE-2022-22025, CVE-2022-22040, CVE-2022-22043, CVE-2022-30208)   - An elevation of privilege vulnerability. An attacker can exploit this to gain elevated privileges.  (CVE-2022-22022, CVE-2022-22026, CVE-2022-22031, CVE-2022-22034, CVE-2022-22036, CVE-2022-22037, CVE-2022-22041, CVE-2022-22045, CVE-2022-22047, CVE-2022-22049, CVE-2022-22050, CVE-2022-30202, CVE-2022-30205, CVE-2022-30206, CVE-2022-30209, CVE-2022-30215, CVE-2022-30220, CVE-2022-30224, CVE-2022-30225, CVE-2022-30226)   - An information disclosure vulnerability. An attacker can exploit this to disclose potentially sensitive information. (CVE-2022-21845, CVE-2022-22028, CVE-2022-22042, CVE-2022-22711, CVE-2022-30213, CVE-2022-30223)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Apply Security Update 5015808 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5015808   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.5246 |

## Security Updates for Microsoft SQL Server (June 2022)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The Microsoft SQL Server installation on the remote host is missing a security update. |
| Description | The Microsoft SQL Server installation on the remote host is missing a security update. It is, therefore, affected by the following vulnerability:   - A remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands. (CVE-2022-29143)  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. |
| Recommendation | Microsoft has released the following security updates to address this issue:   -KB5015371  -KB5014553  -KB5014351  -KB5014353  -KB5014354  -KB5014356  -KB5014365  -KB5014355  -KB5014165  -KB5014164 |
| Evidence | KB : 5014365  - C:\Program Files\Microsoft SQL Server\MSSQL13.VEEAMSQL2016\MSSQL\Binn\sqlservr.exe has not been patched.  Remote version : 2015.131.5026.0  Should be : 2015.131.5108.50   SQL Server Version : 13.0.5026.0 Express Edition  SQL Server Instance : VEEAMSQL2016 |

## KB5013952: Windows 10 Version 1607 and Windows Server 2016 Security Update (May 2022)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5013952. It is, therefore, affected by multiple vulnerabilities   - Windows LDAP Remote Code Execution Vulnerability (CVE-2022-22012, CVE-2022-22013, CVE-2022-22014, CVE-2022-29128, CVE-2022-29129, CVE-2022-29130, CVE-2022-29137, CVE-2022-29139, CVE-2022-29141)   - Windows Network File System Remote Code Execution Vulnerability (CVE-2022-26937)   - Active Directory Domain Services Elevation of Privilege Vulnerability (CVE-2022-26923)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Apply Security Update 5013952 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5013952   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.5125 |

## KB5011495: Windows 10 Version 1607 and Windows Server 2016 Security Update (March 2022)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5011495. It is, therefore, affected by multiple vulnerabilities   - An elevation of privilege vulnerability. An attacker can exploit this to gain elevated privileges.  (CVE-2022-23283, CVE-2022-23284, CVE-2022-23287, CVE-2022-23290, CVE-2022-23293, CVE-2022-23296, CVE-2022-23298, CVE-2022-23299, CVE-2022-24454, CVE-2022-24455, CVE-2022-24459, CVE-2022-24460, CVE-2022-24505, CVE-2022-24507)   - A denial of service (DoS) vulnerability. An attacker can exploit this issue to cause the affected component to deny system or application services. (CVE-2022-21975, CVE-2022-23253)   - A security feature bypass vulnerability exists. An attacker can exploit this and bypass the security feature and perform unauthorized actions compromising the integrity of the system/application.  (CVE-2022-24502)   - An information disclosure vulnerability. An attacker can exploit this to disclose potentially sensitive information. (CVE-2022-21977, CVE-2022-22010, CVE-2022-23281, CVE-2022-23297, CVE-2022-24503)   - A remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands. (CVE-2022-21990, CVE-2022-23285, CVE-2022-23294)  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. |
| Recommendation | Apply Security Update 5011495. |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5011495   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.5006 |

## KB5010359: Windows 10 Version 1607 and Windows Server 2016 Security Update (February 2022)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5010359. It is, therefore, affected by multiple vulnerabilities   - An information disclosure vulnerability. An attacker can exploit this to disclose potentially sensitive information. (CVE-2022-21993, CVE-2022-21998)   - A denial of service (DoS) vulnerability. An attacker can exploit this issue to cause the affected component to deny system or application services. (CVE-2022-22002)   - A remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands. (CVE-2022-21995)   - An elevation of privilege vulnerability. An attacker can exploit this to gain elevated privileges.  (CVE-2022-21989, CVE-2022-21997, CVE-2022-21999, CVE-2022-22000, CVE-2022-22001)  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. |
| Recommendation | Apply Security Update 5010359 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5010359   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.4946 |

## KB5007192: Windows 10 Version 1607 and Windows Server 2016 Security Update (November 2021)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5007192. It is, therefore, affected by multiple vulnerabilities:   - An information disclosure vulnerability. An attacker can exploit this to disclose potentially sensitive information. (CVE-2021-38631, CVE-2021-38665, CVE-2021-41371)   - A remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands. (CVE-2021-38666, CVE-2021-42275, CVE-2021-42276, CVE-2021-42279)   - A denial of service (DoS) vulnerability. An attacker can exploit this issue to cause the affected component to deny system or application services. (CVE-2021-41356, CVE-2021-42274, CVE-2021-42284)   - An elevation of privilege vulnerability. An attacker can exploit this to gain elevated privileges.  (CVE-2021-36957, CVE-2021-41366, CVE-2021-41367, CVE-2021-41370, CVE-2021-41377, CVE-2021-41379, CVE-2021-42277, CVE-2021-42278, CVE-2021-42280, CVE-2021-42282, CVE-2021-42283, CVE-2021-42285, CVE-2021-42287, CVE-2021-42291) |
| Recommendation | Apply Cumulative Update KB5007192. |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5007192   - C:\Windows\system32\gdiplus.dll has not been patched.  Remote version : 10.0.14393.4169  Should be : 10.0.14393.4770 |

## KB5006669: Windows 10 Version 1607 and Windows Server 2016 Security Update (October 2021)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5006669. It is, therefore, affected by multiple vulnerabilities:   - A denial of service (DoS) vulnerability. An attacker can exploit this issue to cause the affected component to deny system or application services. (CVE-2021-36953, CVE-2021-40463)   - An elevation of privilege vulnerability. An attacker can exploit this to gain elevated privileges.  (CVE-2021-26441, CVE-2021-26442, CVE-2021-40443, CVE-2021-40449, CVE-2021-40466, CVE-2021-40467, CVE-2021-40470, CVE-2021-40476, CVE-2021-40477, CVE-2021-40478, CVE-2021-40488, CVE-2021-40489, CVE-2021-41335, CVE-2021-41345, CVE-2021-41347)   - A session spoofing vulnerability exists. An attacker can exploit this to perform actions with the privileges of another user. (CVE-2021-36970, CVE-2021-40455, CVE-2021-41361)   - A remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands. (CVE-2021-40465, CVE-2021-40469, CVE-2021-41331, CVE-2021-41340, CVE-2021-41342)   - An information disclosure vulnerability. An attacker can exploit this to disclose potentially sensitive information. (CVE-2021-38662, CVE-2021-38663, CVE-2021-40454, CVE-2021-41332, CVE-2021-41343)   - A security feature bypass vulnerability exists. An attacker can exploit this and bypass the security feature and perform unauthorized actions compromising the integrity of the system/application.  (CVE-2021-40460, CVE-2021-41337, CVE-2021-41338) |
| Recommendation | Apply Security Update 5006669 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5006669   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.4704 |

## KB5005573: Windows 10 Version 1607 and Windows Server 2016 September 2021 Security Update

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The remote Windows host is affected by multiple vulnerabilities. |
| Description | The remote Windows host is missing security update 5005573. It is, therefore, affected by multiple vulnerabilities :   - An memory corruption vulnerability exists. An attacker can exploit this to corrupt the memory and cause unexpected behaviors within the system/application.  (CVE-2021-26435)   - An information disclosure vulnerability. An attacker can exploit this to disclose potentially sensitive information. (CVE-2021-36960, CVE-2021-36962, CVE-2021-36969, CVE-2021-36972, CVE-2021-38629, CVE-2021-38635, CVE-2021-38636)   - A security feature bypass vulnerability exists. An attacker can exploit this and bypass the security feature and perform unauthorized actions compromising the integrity of the system/application.  (CVE-2021-38624, CVE-2021-38632)   - An elevation of privilege vulnerability. An attacker can exploit this to gain elevated privileges.  (CVE-2021-36955, CVE-2021-36963, CVE-2021-36964, CVE-2021-36967, CVE-2021-36973, CVE-2021-36974, CVE-2021-38628, CVE-2021-38630, CVE-2021-38633, CVE-2021-38634, CVE-2021-38638, CVE-2021-38639, CVE-2021-38667, CVE-2021-38671, CVE-2021-40447)   - A remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands. (CVE-2021-36965, CVE-2021-36958, CVE-2021-40444)   - A denial of service (DoS) vulnerability. An attacker can exploit this issue to cause the affected component to deny system or application services. (CVE-2021-36961)   - A session spoofing vulnerability exists. An attacker can exploit this to perform actions with the privileges of another user. (CVE-2021-36959) |
| Recommendation | Apply Cumulative Update KB5005573. |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5005573   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.4651 |

## KB5004948: Windows 10 1607 and Windows Server 2016 OOB Security Update RCE (July 2021)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The remote Windows host is affected by a remote code execution vulnerability. |
| Description | A remote command execution vulnerability exists in Windows Print Spooler service improperly performs privileged file operations. An authenticated, remote attacker can exploit this to bypass and run arbitrary code with SYSTEM privileges. |
| Recommendation | Apply Cumulative Update 5004948 |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5004948   - C:\Windows\system32\localspl.dll has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.4470 |

## KB5001347: Windows 10 version 1607 / Windows Server 2016 Security Update (Apr 2021)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The remote host is missing one or more security updates. |
| Description | The remote Windows host is missing security updates. It is, therefore, affected by multiple vulnerabilities:   - Win32k Elevation of Privilege Vulnerability (CVE-2021-27072)   - Windows Media Photo Codec Information Disclosure Vulnerability (CVE-2021-27079)   - Microsoft Internet Messaging API Remote Code Execution Vulnerability (CVE-2021-27089)   - Windows Kernel Information Disclosure Vulnerability (CVE-2021-27093, CVE-2021-28309)   - Windows Early Launch Antimalware Driver Security Feature Bypass Vulnerability (CVE-2021-27094, CVE-2021-28447)   - Windows Media Video Decoder Remote Code Execution Vulnerability (CVE-2021-27095, CVE-2021-28315)   - NTFS Elevation of Privilege Vulnerability (CVE-2021-27096)   - Windows Installer Spoofing Vulnerability (CVE-2021-26413)   - Windows Installer Elevation of Privilege Vulnerability (CVE-2021-26415, CVE-2021-28440)   - Windows Hyper-V Denial of Service Vulnerability (CVE-2021-26416)   - Windows Application Compatibility Cache Denial of Service Vulnerability (CVE-2021-28311)   - Windows WLAN AutoConfig Service Security Feature Bypass Vulnerability (CVE-2021-28316)   - Microsoft Windows Codecs Library Information Disclosure Vulnerability (CVE-2021-28317)   - Windows GDI+ Information Disclosure Vulnerability (CVE-2021-28318)   - Windows Resource Manager PSM Service Extension Elevation of Privilege Vulnerability (CVE-2021-28320)   - Windows DNS Information Disclosure Vulnerability (CVE-2021-28323, CVE-2021-28328)   - Windows SMB Information Disclosure Vulnerability (CVE-2021-28325)   - Windows AppX Deployment Server Denial of Service Vulnerability (CVE-2021-28326)   - Remote Procedure Call Runtime Remote Code Execution Vulnerability (CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434)   - Windows Speech Runtime Elevation of Privilege Vulnerability (CVE-2021-28347, CVE-2021-28351, CVE-2021-28436)   - Windows GDI+ Remote Code Execution Vulnerability (CVE-2021-28348, CVE-2021-28349, CVE-2021-28350)   - Windows Event Tracing Information Disclosure Vulnerability (CVE-2021-28435)   - Windows Installer Information Disclosure Vulnerability (CVE-2021-28437)   - Windows TCP/IP Driver Denial of Service Vulnerability (CVE-2021-28439)   - Windows Console Driver Denial of Service Vulnerability (CVE-2021-28443)   - Windows Hyper-V Security Feature Bypass Vulnerability (CVE-2021-28444)   - N/A (CVE-2021-28445, CVE-2021-28446)  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. |
| Recommendation | Microsoft has released KB5001347 to address this issue. |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5001347   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.4350 |

## Security Updates for Microsoft SQL Server (January 2021)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The Microsoft SQL Server installation on the remote host is missing a security update. |
| Description | The Microsoft SQL Server installation on the remote host is missing a security update. It is, therefore, affected by an elevation of privilege vulnerability. An authenticated, remote attacker can exploit this issue, to gain elevated privileges.  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. |
| Recommendation | Microsoft has released the following security updates to address this issue:  -KB4583456  -KB4583457  -KB4583458  -KB4583459  -KB4583460  -KB4583461  -KB4583462  -KB4583463  -KB4583465 |
| Evidence | KB : 4583460  - C:\Program Files\Microsoft SQL Server\MSSQL13.VEEAMSQL2016\MSSQL\Binn\sqlservr.exe has not been patched.  Remote version : 2015.131.5026.0  Should be : 2015.131.5103.6   SQL Server Version : 13.0.5026.0 Express Edition  SQL Server Instance : VEEAMSQL2016 |

## Security Updates for Microsoft .NET core (May 2022)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The Microsoft .NET core installations on the remote host are affected by multiple vulnerabilities. |
| Description | The Microsoft .NET core installations on the remote host are missing security updates. It is, therefore, affected by multiple denial of service vulnerabilities:   - A vulnerability where a malicious client can cause a denial of service via excess memory allocations through HttpClient. (CVE-2022-23267)   - A vulnerability where a malicious client can manipulate cookies and cause a denial of service. (CVE-2022-29117)   - A vulnerability where a malicious client can cause a denial of service when HTML forms are parsed. (CVE-2022-29145)  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. |
| Recommendation | Update .NET Core Runtime to version 3.1.25, 5.0.17 or 6.0.5. |
| Evidence | Path : C:\Program Files\dotnet\shared\Microsoft.NetCore.App\3.1.16\  Installed version : 3.1.16.30112  Fixed version : 3.1.25 |

## Google Chrome < 131.0.6778.108 Vulnerability

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | A web browser installed on the remote Windows host is affected by a vulnerability. |
| Description | The version of Google Chrome installed on the remote Windows host is prior to 131.0.6778.108. It is, therefore, affected by a vulnerability as referenced in the 2024\_12\_stable-channel-update-for-desktop advisory.   - Type Confusion in V8. (CVE-2024-12053)  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to Google Chrome version 131.0.6778.108 or later. |
| Evidence | Path : C:\Program Files\Google\Chrome\Application  Installed version : 126.0.6478.128  Fixed version : 131.0.6778.108 |

## Google Chrome < 131.0.6778.85 Vulnerability

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | A web browser installed on the remote Windows host is affected by a vulnerability. |
| Description | The version of Google Chrome installed on the remote Windows host is prior to 131.0.6778.85. It is, therefore, affected by a vulnerability as referenced in the 2024\_11\_stable-channel-update-for-desktop\_19 advisory.   - Type Confusion in V8. (CVE-2024-11395)  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to Google Chrome version 131.0.6778.85 or later. |
| Evidence | Path : C:\Program Files\Google\Chrome\Application  Installed version : 126.0.6478.128  Fixed version : 131.0.6778.85 |

## Google Chrome < 131.0.6778.69 Multiple Vulnerabilities

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | A web browser installed on the remote Windows host is affected by multiple vulnerabilities. |
| Description | The version of Google Chrome installed on the remote Windows host is prior to 131.0.6778.69. It is, therefore, affected by multiple vulnerabilities as referenced in the 2024\_11\_stable-channel-update-for-desktop\_12 advisory.   - Inappropriate implementation in Blink. (CVE-2024-11110)   - Inappropriate implementation in Autofill. (CVE-2024-11111)   - Use after free in Media. (CVE-2024-11112)   - Use after free in Accessibility. (CVE-2024-11113)   - Inappropriate implementation in Views. (CVE-2024-11114)   - Insufficient policy enforcement in Navigation. (CVE-2024-11115)   - Inappropriate implementation in Paint. (CVE-2024-11116)   - Inappropriate implementation in FileSystem. (CVE-2024-11117)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to Google Chrome version 131.0.6778.69 or later. |
| Evidence | Path : C:\Program Files\Google\Chrome\Application  Installed version : 126.0.6478.128  Fixed version : 131.0.6778.69 |

## Google Chrome < 130.0.6723.116 Multiple Vulnerabilities

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | A web browser installed on the remote Windows host is affected by multiple vulnerabilities. |
| Description | The version of Google Chrome installed on the remote Windows host is prior to 130.0.6723.116. It is, therefore, affected by multiple vulnerabilities as referenced in the 2024\_11\_stable-channel-update-for-desktop advisory.   - Use after free in Family Experiences. (CVE-2024-10826)   - Use after free in Serial. (CVE-2024-10827)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to Google Chrome version 130.0.6723.116 or later. |
| Evidence | Path : C:\Program Files\Google\Chrome\Application  Installed version : 126.0.6478.128  Fixed version : 130.0.6723.116 |

## Google Chrome < 130.0.6723.117 Multiple Vulnerabilities

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | A web browser installed on the remote Windows host is affected by multiple vulnerabilities. |
| Description | The version of Google Chrome installed on the remote Windows host is prior to 130.0.6723.117. It is, therefore, affected by multiple vulnerabilities as referenced in the 2024\_11\_stable-channel-update-for-desktop advisory.   - Use after free in Family Experiences. (CVE-2024-10826)   - Use after free in Serial. (CVE-2024-10827)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to Google Chrome version 130.0.6723.117 or later. |
| Evidence | Path : C:\Program Files\Google\Chrome\Application  Installed version : 126.0.6478.128  Fixed version : 130.0.6723.117 |

## Google Chrome < 130.0.6723.92 Multiple Vulnerabilities

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | A web browser installed on the remote Windows host is affected by multiple vulnerabilities. |
| Description | The version of Google Chrome installed on the remote Windows host is prior to 130.0.6723.92. It is, therefore, affected by multiple vulnerabilities as referenced in the 2024\_10\_stable-channel-update-for-desktop\_29 advisory.   - Out of bounds write in Dawn. (CVE-2024-10487)   - Use after free in WebRTC. (CVE-2024-10488)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to Google Chrome version 130.0.6723.92 or later. |
| Evidence | Path : C:\Program Files\Google\Chrome\Application  Installed version : 126.0.6478.128  Fixed version : 130.0.6723.92 |

## Google Chrome < 130.0.6723.91 Multiple Vulnerabilities

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | A web browser installed on the remote Windows host is affected by multiple vulnerabilities. |
| Description | The version of Google Chrome installed on the remote Windows host is prior to 130.0.6723.91. It is, therefore, affected by multiple vulnerabilities as referenced in the 2024\_10\_stable-channel-update-for-desktop\_29 advisory.   - Out of bounds write in Dawn. (CVE-2024-10487)   - Use after free in WebRTC. (CVE-2024-10488)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to Google Chrome version 130.0.6723.91 or later. |
| Evidence | Path : C:\Program Files\Google\Chrome\Application  Installed version : 126.0.6478.128  Fixed version : 130.0.6723.91 |

## Google Chrome < 130.0.6723.70 Multiple Vulnerabilities

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | A web browser installed on the remote Windows host is affected by multiple vulnerabilities. |
| Description | The version of Google Chrome installed on the remote Windows host is prior to 130.0.6723.70. It is, therefore, affected by multiple vulnerabilities as referenced in the 2024\_10\_stable-channel-update-for-desktop\_22 advisory.   - Inappropriate implementation in Extensions. (CVE-2024-10229)   - Type Confusion in V8. (CVE-2024-10230, CVE-2024-10231)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to Google Chrome version 130.0.6723.70 or later. |
| Evidence | Path : C:\Program Files\Google\Chrome\Application  Installed version : 126.0.6478.128  Fixed version : 130.0.6723.70 |

## Google Chrome < 130.0.6723.69 Multiple Vulnerabilities

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | A web browser installed on the remote Windows host is affected by multiple vulnerabilities. |
| Description | The version of Google Chrome installed on the remote Windows host is prior to 130.0.6723.69. It is, therefore, affected by multiple vulnerabilities as referenced in the 2024\_10\_stable-channel-update-for-desktop\_22 advisory.   - Inappropriate implementation in Extensions. (CVE-2024-10229)   - Type Confusion in V8. (CVE-2024-10230, CVE-2024-10231)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to Google Chrome version 130.0.6723.69 or later. |
| Evidence | Path : C:\Program Files\Google\Chrome\Application  Installed version : 126.0.6478.128  Fixed version : 130.0.6723.69 |

## Google Chrome < 130.0.6723.58 Multiple Vulnerabilities

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | A web browser installed on the remote Windows host is affected by multiple vulnerabilities. |
| Description | The version of Google Chrome installed on the remote Windows host is prior to 130.0.6723.58. It is, therefore, affected by multiple vulnerabilities as referenced in the 2024\_10\_stable-channel-update-for-desktop\_15 advisory.   - Use after free in AI. (CVE-2024-9954)   - Use after free in Web Authentication. (CVE-2024-9955)   - Inappropriate implementation in Web Authentication. (CVE-2024-9956)   - Use after free in UI. (CVE-2024-9957)   - Inappropriate implementation in PictureInPicture. (CVE-2024-9958)   - Use after free in DevTools. (CVE-2024-9959)   - Use after free in Dawn. (CVE-2024-9960)   - Use after free in Parcel Tracking. (CVE-2024-9961)   - Inappropriate implementation in Permissions. (CVE-2024-9962)   - Insufficient data validation in Downloads. (CVE-2024-9963)   - Inappropriate implementation in Payments. (CVE-2024-9964)   - Insufficient data validation in DevTools. (CVE-2024-9965)   - Inappropriate implementation in Navigations. (CVE-2024-9966)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to Google Chrome version 130.0.6723.58 or later. |
| Evidence | Path : C:\Program Files\Google\Chrome\Application  Installed version : 126.0.6478.128  Fixed version : 130.0.6723.58 |

## Google Chrome < 130.0.6723.59 Multiple Vulnerabilities

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | A web browser installed on the remote Windows host is affected by multiple vulnerabilities. |
| Description | The version of Google Chrome installed on the remote Windows host is prior to 130.0.6723.59. It is, therefore, affected by multiple vulnerabilities as referenced in the 2024\_10\_stable-channel-update-for-desktop\_15 advisory.   - Use after free in AI. (CVE-2024-9954)   - Use after free in Web Authentication. (CVE-2024-9955)   - Inappropriate implementation in Web Authentication. (CVE-2024-9956)   - Use after free in UI. (CVE-2024-9957)   - Inappropriate implementation in PictureInPicture. (CVE-2024-9958)   - Use after free in DevTools. (CVE-2024-9959)   - Use after free in Dawn. (CVE-2024-9960)   - Use after free in Parcel Tracking. (CVE-2024-9961)   - Inappropriate implementation in Permissions. (CVE-2024-9962)   - Insufficient data validation in Downloads. (CVE-2024-9963)   - Inappropriate implementation in Payments. (CVE-2024-9964)   - Insufficient data validation in DevTools. (CVE-2024-9965)   - Inappropriate implementation in Navigations. (CVE-2024-9966)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to Google Chrome version 130.0.6723.59 or later. |
| Evidence | Path : C:\Program Files\Google\Chrome\Application  Installed version : 126.0.6478.128  Fixed version : 130.0.6723.59 |

## Security Update for Microsoft .NET Core (July 2024)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The remote Windows host is affected by a .NET Core vulnerability |
| Description | The version of tested product installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the vendor advisory.   - .NET, .NET Framework, and Visual Studio Elevation of Privilege Vulnerability (CVE-2024-38081)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Update .NET Core, remove vulnerable packages and refer to vendor advisory. |
| Evidence | Path : C:\Program Files\dotnet\shared\Microsoft.NetCore.App\6.0.25\  Installed version : 6.0.25.33020  Fixed version : 6.0.32 |

## Security Update for Microsoft .NET Core (October 2024)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The remote Windows host is affected by a .NET Core vulnerability |
| Description | The version of tested product installed on the remote host is prior to tested version. It is, therefore, affected by multiple vulnerabilities as referenced in the vendor advisory.   - .NET and Visual Studio Remote Code Execution Vulnerability (CVE-2024-38229)   - .NET and Visual Studio Denial of Service Vulnerability (CVE-2024-43483,CVE-2024-43484,CVE-2024-43485)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Update .NET Core, remove vulnerable packages and refer to vendor advisory. |
| Evidence | Path : C:\Program Files\dotnet\shared\Microsoft.NetCore.App\6.0.25\  Installed version : 6.0.25.33020  Fixed version : 6.0.35 |

## Google Chrome < 129.0.6668.100 Multiple Vulnerabilities

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | A web browser installed on the remote Windows host is affected by multiple vulnerabilities. |
| Description | The version of Google Chrome installed on the remote Windows host is prior to 129.0.6668.100. It is, therefore, affected by multiple vulnerabilities as referenced in the 2024\_10\_stable-channel-update-for-desktop\_8 advisory.   - Type Confusion in V8. (CVE-2024-9602, CVE-2024-9603)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to Google Chrome version 129.0.6668.100 or later. |
| Evidence | Path : C:\Program Files\Google\Chrome\Application  Installed version : 126.0.6478.128  Fixed version : 129.0.6668.100 |

## Google Chrome < 129.0.6668.89 Multiple Vulnerabilities

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | A web browser installed on the remote Windows host is affected by multiple vulnerabilities. |
| Description | The version of Google Chrome installed on the remote Windows host is prior to 129.0.6668.89. It is, therefore, affected by multiple vulnerabilities as referenced in the 2024\_10\_stable-channel-update-for-desktop advisory.   - Integer overflow in Layout. (CVE-2024-7025)   - Insufficient data validation in Mojo. (CVE-2024-9369)   - Inappropriate implementation in V8. (CVE-2024-9370)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to Google Chrome version 129.0.6668.89 or later. |
| Evidence | Path : C:\Program Files\Google\Chrome\Application  Installed version : 126.0.6478.128  Fixed version : 129.0.6668.89 |

## Google Chrome < 129.0.6668.70 Multiple Vulnerabilities

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | A web browser installed on the remote Windows host is affected by multiple vulnerabilities. |
| Description | The version of Google Chrome installed on the remote Windows host is prior to 129.0.6668.70. It is, therefore, affected by multiple vulnerabilities as referenced in the 2024\_09\_stable-channel-update-for-desktop\_24 advisory.   - Use after free in Dawn. (CVE-2024-9120)   - Inappropriate implementation in V8. (CVE-2024-9121)   - Type Confusion in V8. (CVE-2024-9122)   - Integer overflow in Skia. (CVE-2024-9123)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to Google Chrome version 129.0.6668.70 or later. |
| Evidence | Path : C:\Program Files\Google\Chrome\Application  Installed version : 126.0.6478.128  Fixed version : 129.0.6668.70 |

## Google Chrome < 128.0.6613.137 Multiple Vulnerabilities

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | A web browser installed on the remote Windows host is affected by multiple vulnerabilities. |
| Description | The version of Google Chrome installed on the remote Windows host is prior to 128.0.6613.137. It is, therefore, affected by multiple vulnerabilities as referenced in the 2024\_09\_stable-channel-update-for-desktop\_10 advisory.   - Heap buffer overflow in Skia in Google Chrome prior to 128.0.6613.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-8636)   - Use after free in Media Router in Google Chrome on Android prior to 128.0.6613.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity:  High) (CVE-2024-8637)   - Type Confusion in V8 in Google Chrome prior to 128.0.6613.137 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-8638)   - Use after free in Autofill in Google Chrome on Android prior to 128.0.6613.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-8639)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to Google Chrome version 128.0.6613.137 or later. |
| Evidence | Path : C:\Program Files\Google\Chrome\Application  Installed version : 126.0.6478.128  Fixed version : 128.0.6613.137 |

## Google Chrome < 128.0.6613.138 Multiple Vulnerabilities

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | A web browser installed on the remote Windows host is affected by multiple vulnerabilities. |
| Description | The version of Google Chrome installed on the remote Windows host is prior to 128.0.6613.138. It is, therefore, affected by multiple vulnerabilities as referenced in the 2024\_09\_stable-channel-update-for-desktop\_10 advisory.   - Heap buffer overflow in Skia in Google Chrome prior to 128.0.6613.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-8636)   - Use after free in Media Router in Google Chrome on Android prior to 128.0.6613.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity:  High) (CVE-2024-8637)   - Type Confusion in V8 in Google Chrome prior to 128.0.6613.137 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-8638)   - Use after free in Autofill in Google Chrome on Android prior to 128.0.6613.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-8639)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to Google Chrome version 128.0.6613.138 or later. |
| Evidence | Path : C:\Program Files\Google\Chrome\Application  Installed version : 126.0.6478.128  Fixed version : 128.0.6613.138 |

## Google Chrome < 128.0.6613.119 Multiple Vulnerabilities

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | A web browser installed on the remote Windows host is affected by multiple vulnerabilities. |
| Description | The version of Google Chrome installed on the remote Windows host is prior to 128.0.6613.119. It is, therefore, affected by multiple vulnerabilities as referenced in the 2024\_09\_stable-channel-update-for-desktop advisory.   - Use after free in WebAudio in Google Chrome prior to 128.0.6613.119 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-8362)   - Out of bounds write in V8 in Google Chrome prior to 128.0.6613.119 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-7970)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to Google Chrome version 128.0.6613.119 or later. |
| Evidence | Path : C:\Program Files\Google\Chrome\Application  Installed version : 126.0.6478.128  Fixed version : 128.0.6613.119 |

## Google Chrome < 128.0.6613.120 Multiple Vulnerabilities

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | A web browser installed on the remote Windows host is affected by multiple vulnerabilities. |
| Description | The version of Google Chrome installed on the remote Windows host is prior to 128.0.6613.120. It is, therefore, affected by multiple vulnerabilities as referenced in the 2024\_09\_stable-channel-update-for-desktop advisory.   - Use after free in WebAudio in Google Chrome prior to 128.0.6613.119 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-8362)   - Out of bounds write in V8 in Google Chrome prior to 128.0.6613.119 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-7970)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to Google Chrome version 128.0.6613.120 or later. |
| Evidence | Path : C:\Program Files\Google\Chrome\Application  Installed version : 126.0.6478.128  Fixed version : 128.0.6613.120 |

## Google Chrome < 128.0.6613.113 Multiple Vulnerabilities

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | A web browser installed on the remote Windows host is affected by multiple vulnerabilities. |
| Description | The version of Google Chrome installed on the remote Windows host is prior to 128.0.6613.113. It is, therefore, affected by multiple vulnerabilities as referenced in the 2024\_08\_stable-channel-update-for-desktop\_28 advisory.   - Type Confusion in V8 in Google Chrome prior to 128.0.6613.113 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-7969, CVE-2024-8194)   - Heap buffer overflow in Skia in Google Chrome prior to 128.0.6613.113 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-8193, CVE-2024-8198)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to Google Chrome version 128.0.6613.113 or later. |
| Evidence | Path : C:\Program Files\Google\Chrome\Application  Installed version : 126.0.6478.128  Fixed version : 128.0.6613.113 |

## Google Chrome < 128.0.6613.114 Multiple Vulnerabilities

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | A web browser installed on the remote Windows host is affected by multiple vulnerabilities. |
| Description | The version of Google Chrome installed on the remote Windows host is prior to 128.0.6613.114. It is, therefore, affected by multiple vulnerabilities as referenced in the 2024\_08\_stable-channel-update-for-desktop\_28 advisory.   - Type Confusion in V8 in Google Chrome prior to 128.0.6613.113 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-7969, CVE-2024-8194)   - Heap buffer overflow in Skia in Google Chrome prior to 128.0.6613.113 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-8193, CVE-2024-8198)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to Google Chrome version 128.0.6613.114 or later. |
| Evidence | Path : C:\Program Files\Google\Chrome\Application  Installed version : 126.0.6478.128  Fixed version : 128.0.6613.114 |

## Google Chrome < 127.0.6533.99 Multiple Vulnerabilities

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | A web browser installed on the remote Windows host is affected by multiple vulnerabilities. |
| Description | The version of Google Chrome installed on the remote Windows host is prior to 127.0.6533.99. It is, therefore, affected by multiple vulnerabilities as referenced in the 2024\_08\_stable-channel-update-for-desktop advisory.   - Out of bounds memory access in ANGLE in Google Chrome prior to 127.0.6533.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical) (CVE-2024-7532)   - Use after free in Sharing in Google Chrome on iOS prior to 127.0.6533.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-7533)   - Type Confusion in V8 in Google Chrome prior to 127.0.6533.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-7550)   - Heap buffer overflow in Layout in Google Chrome prior to 127.0.6533.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-7534)   - Inappropriate implementation in V8 in Google Chrome prior to 127.0.6533.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-7535)   - Use after free in WebAudio in Google Chrome prior to 127.0.6533.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-7536)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to Google Chrome version 127.0.6533.99 or later. |
| Evidence | Path : C:\Program Files\Google\Chrome\Application  Installed version : 126.0.6478.128  Fixed version : 127.0.6533.99 |

## Google Chrome < 127.0.6533.88 Multiple Vulnerabilities

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | A web browser installed on the remote Windows host is affected by multiple vulnerabilities. |
| Description | The version of Google Chrome installed on the remote Windows host is prior to 127.0.6533.88. It is, therefore, affected by multiple vulnerabilities as referenced in the 2024\_07\_stable-channel-update-for-desktop\_30 advisory.   - Uninitialized Use in Dawn. (CVE-2024-6990)   - Out of bounds read in WebTransport. (CVE-2024-7255)   - Insufficient data validation in Dawn. (CVE-2024-7256)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to Google Chrome version 127.0.6533.88 or later. |
| Evidence | Path : C:\Program Files\Google\Chrome\Application  Installed version : 126.0.6478.128  Fixed version : 127.0.6533.88 |

## Google Chrome < 127.0.6533.72 Multiple Vulnerabilities

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | A web browser installed on the remote Windows host is affected by multiple vulnerabilities. |
| Description | The version of Google Chrome installed on the remote Windows host is prior to 127.0.6533.72. It is, therefore, affected by multiple vulnerabilities as referenced in the 2024\_07\_stable-channel-update-for-desktop\_23 advisory.   - Use after free in Downloads. (CVE-2024-6988)   - Use after free in Loader. (CVE-2024-6989)   - Use after free in Dawn. (CVE-2024-6991)   - Heap buffer overflow in Layout. (CVE-2024-6994)   - Inappropriate implementation in Fullscreen. (CVE-2024-6995)   - Use after free in Tabs. (CVE-2024-6997)   - Use after free in User Education. (CVE-2024-6998)   - Inappropriate implementation in FedCM. (CVE-2024-6999, CVE-2024-7003)   - Use after free in CSS. (CVE-2024-7000)   - Inappropriate implementation in HTML. (CVE-2024-7001)   - Insufficient validation of untrusted input in Safe Browsing. (CVE-2024-7004, CVE-2024-7005)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to Google Chrome version 127.0.6533.72 or later. |
| Evidence | Path : C:\Program Files\Google\Chrome\Application  Installed version : 126.0.6478.128  Fixed version : 127.0.6533.72 |

## Google Chrome < 126.0.6478.182 Multiple Vulnerabilities

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | A web browser installed on the remote Windows host is affected by multiple vulnerabilities. |
| Description | The version of Google Chrome installed on the remote Windows host is prior to 126.0.6478.182. It is, therefore, affected by multiple vulnerabilities as referenced in the 2024\_07\_stable-channel-update-for-desktop advisory.   - Inappropriate implementation in V8 in Google Chrome prior to 126.0.6478.182 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High) (CVE-2024-6772)   - Inappropriate implementation in V8 in Google Chrome prior to 126.0.6478.182 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-6773)   - Use after free in Screen Capture in Google Chrome prior to 126.0.6478.182 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-6774)   - Use after free in Media Stream in Google Chrome prior to 126.0.6478.182 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-6775)   - Use after free in Audio in Google Chrome prior to 126.0.6478.182 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-6776)   - Use after free in Navigation in Google Chrome prior to 126.0.6478.182 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension. (Chromium security severity: High) (CVE-2024-6777)   - Race in DevTools in Google Chrome prior to 126.0.6478.182 allowed an attacker who convinced a user to install a malicious extension to inject scripts or HTML into a privileged page via a crafted Chrome Extension. (Chromium security severity: High) (CVE-2024-6778)   - Out of bounds memory access in V8 in Google Chrome prior to 126.0.6478.182 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High) (CVE-2024-6779)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to Google Chrome version 126.0.6478.182 or later. |
| Evidence | Path : C:\Program Files\Google\Chrome\Application  Installed version : 126.0.6478.128  Fixed version : 126.0.6478.182 |

## PuTTY < 0.81 Key Recovery Attack Vulnerability

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The remote Windows host has an SSH client that is affected by an key recovery attack vulnerability. |
| Description | In PuTTY 0.68 through 0.80 before 0.81, biased ECDSA nonce generation allows an attacker to recover a user's NIST P-521 secret key via a quick attack in approximately 60 signatures. This is especially important in a scenario where an adversary is able to read messages signed by PuTTY or Pageant. The required set of signed messages may be publicly readable because they are stored in a public Git service that supports use of SSH for commit signing, and the signatures were made by Pageant through an agent-forwarding mechanism. In other words, an adversary may already have enough signature information to compromise a victim's private key, even if there is no further use of vulnerable PuTTY versions. After a key compromise, an adversary may be able to conduct supply-chain attacks on software maintained in Git. A second, independent scenario is that the adversary is an operator of an SSH server to which the victim authenticates (for remote login or file copy), even though this server is not fully trusted by the victim, and the victim uses the same private key for SSH connections to other services operated by other entities. Here, the rogue server operator (who would otherwise have no way to determine the victim's private key) can derive the victim's private key, and then use it for unauthorized access to those other services. If the other services include Git services, then again it may be possible to conduct supply-chain attacks on software maintained in Git.   Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to PuTTY version 0.81 or later. |
| Evidence | Path : C:\Program Files\PuTTY  Installed version : 0.76.0.0  Fixed version : 0.81 |

## Security Update for Microsoft .NET Core (April 2024)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The remote Windows host is affected by a .NET Core vulnerability |
| Description | The version of tested product installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the 2024\_Apr\_09 advisory.   - .NET, .NET Framework, and Visual Studio Remote Code Execution Vulnerability (CVE-2024-21409)  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. |
| Recommendation | Update .NET Core, remove vulnerable packages and refer to vendor advisory. |
| Evidence | Path : C:\Program Files\dotnet\shared\Microsoft.NetCore.App\6.0.25\  Installed version : 6.0.25.33020  Fixed version : 6.0.29 |

## Security Update for Microsoft .NET Core (February 2024)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The remote Windows host is affected by a .NET Core vulnerability |
| Description | The version of tested product installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the 2024\_Feb\_13 advisory.   - .NET Denial of Service Vulnerability (CVE-2024-21404)  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. |
| Recommendation | Update .NET Core, remove vulnerable packages and refer to vendor advisory. |
| Evidence | Path : C:\Program Files\dotnet\shared\Microsoft.NetCore.App\6.0.25\  Installed version : 6.0.25.33020  Fixed version : 6.0.27 |

## VMware Tools 10.3.x / 11.x / 12.x < 12.3.5 Token Bypass (VMSA-2023-0024)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The virtualization tool suite is installed on the remote Windows host is affected by an authentication bypass vulnerability. |
| Description | The version of VMware Tools installed on the remote Windows host is 10.3.x, 11.x or 12.x prior to 12.3.5. It is, therefore, affected by a SAML token signature bypass vulnerability. A malicious actor that has been granted Guest Operation Privileges in a target virtual machine may be able to elevate their privileges if that target virtual machine has been assigned a more privileged Guest Alias.  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to VMware Tools version 12.3.5 or later. |
| Evidence | Path : C:\Program Files\VMware\VMware Tools\  Installed version : 11.0.1.15528  Fixed version : 12.3.5 |

## VMware Tools 10.3.x / 11.x / 12.x < 12.3.0 Authentication Bypass (VMSA-2023-0019)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The virtualization tool suite is installed on the remote Windows host is affected by an authentication bypass vulnerability. |
| Description | The version of VMware Tools installed on the remote Windows host is 10.3.x, 11.x or 12.x prior to 12.3.0. It is, therefore, affected by a SAML token signature bypass vulnerability. A malicious attacker with man-in-the-middle network positioning in the virtual machine network can bypass SAML token signature verification resulting in being able to perform VMware Tools Guest Operations.  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to VMware Tools version 12.3.0 or later. |
| Evidence | Path : C:\Program Files\VMware\VMware Tools\  Installed version : 11.0.1.15528  Fixed version : 12.3.0 |

## Security Updates for Microsoft .NET Core (December 2022)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The Microsoft .NET core installations on the remote host are affected by remote code execution vulnerability. |
| Description | A remote code execution vulnerability exists in .NET Core 3.1, .NET 6.0, and .NET 7.0, where a malicious actor could cause a user to run arbitrary code as a result of parsing maliciously crafted xps files.  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. |
| Recommendation | Update .NET Core Runtime to version 3.1.32 or 6.0.12 or 7.0.1. |
| Evidence | Path : C:\Program Files\dotnet\shared\Microsoft.NetCore.App\3.1.16\  Installed version : 3.1.16.30112  Fixed version : 3.1.32 |

## Security Updates for Microsoft .NET Core (October 2022)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The Microsoft .NET core installations on the remote host are affected by a privilege escalation vulnerability. |
| Description | A privilege escalation vulnerability exists in .NET core 6.0 < 6.0.10 and .NET Core 3.1 < 3.1.30. An authenticated, local attacker can exploit this, via the NuGet client, to cause the user to execute arbitrary code.  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. |
| Recommendation | Update .NET Core Runtime to version 3.1.30 or 6.0.10. |
| Evidence | Path : C:\Program Files\dotnet\shared\Microsoft.NetCore.App\3.1.16\  Installed version : 3.1.16.30112  Fixed version : 3.1.30 |

## Security Updates for Microsoft .NET Core (September 2022)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The Microsoft .NET core installations on the remote host are affected by a denial of service vulnerability. |
| Description | A denial of service vulnerability exists in .NET core 6.0 < 6.0.9 and .NET Core 3.1 < 3.1.29. An unauthenticated, remote attacker can exploit this, by sending a customized payload that is parsed during model binding, to cause a stack overflow, which may cause the application to stop responding.  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. |
| Recommendation | Update .NET Core Runtime to version 3.1.29 or 6.0.9. |
| Evidence | Path : C:\Program Files\dotnet\shared\Microsoft.NetCore.App\3.1.16\  Installed version : 3.1.16.30112  Fixed version : 3.1.29 |

## VMware Tools 11.x / 12.x < 12.1.0 Privilege Escalation (VMSA-2022-0024)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | A virtualization tool suite is installed on the remote Windows host is affected by a privilege escalation vulnerability. |
| Description | The version of VMware Tools installed on the remote Windows host is affected by a privilege escalation vulnerability. A malicious actor with local non-administrative access to the Guest OS can escalate privileges as a root user in the virtual machine.  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to VMware Tools version 12.1.0 or later. |
| Evidence | Path : C:\Program Files\VMware\VMware Tools\  Installed version : 11.0.1.15528  Fixed version : 12.1.0 |

## VMware Tools 10.x / 11.x / 12.x < 12.0.5 XXE (VMSA-2022-0015)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | A virtualization tool suite is installed on the remote Windows host is affected by an XML External Entity vulnerability. |
| Description | The version of VMware Tools installed on the remote Windows host is affected by an XML External Entity (XXE) vulnerability. A malicious actor with non-administrative local user privileges in the Windows guest OS, where VMware Tools is installed, may exploit this issue leading to a denial-of-service condition or unintended information disclosure.  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to VMware Tools version 12.0.5 or later. |
| Evidence | Path : C:\Program Files\VMware\VMware Tools\  Installed version : 11.0.1.15528  Fixed version : 12.0.5 |

## Security Updates for Microsoft ASP.NET Core (December 2021)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The Microsoft ASP.NET Core installations on the remote host are missing a security update. |
| Description | The Microsoft ASP.NET Core installations on the remote host are missing a security update. It is, therefore, affected by an elevation of privilege vulnerability. An attacker can exploit this to gain elevated privileges.  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. |
| Recommendation | Update ASP.NET Core, remove vulnerable packages and refer to vendor advisory. |
| Evidence | Path : C:\Program Files\dotnet\shared\Microsoft.AspNetCore.App\3.1.16  Installed version : 3.1.16  Fixed version : 3.1.22 |

## Security Update for .NET Core (August 2021)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | The remote Windows host is affected by a .NET Core denial of service (DoS) vulnerability. |
| Description | The Microsoft .NET Core installation on the remote host is version 2.1.x prior to 2.1.29, 3.1.x prior to 3.1.18, or 5.x prior to 5.0.9. It is, therefore affected by a denial of service (DoS) vulnerability, as server applications providing WebSocket endpoints can be tricked into endlessly looping while trying to read a single WebSocket frame.  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. |
| Recommendation | Update .NET Core, remove vulnerable packages and refer to vendor advisory. |
| Evidence | Path : C:\Program Files\dotnet\shared\Microsoft.NetCore.App\3.1.16\  Installed version : 3.1.16.30112  Fixed version : 3.1.18 |

## VMware Tools 11.x < 11.2.6 Privilege Escalation (VMSA-2021-0013)

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | A virtualization tool suite installed on the remote Windows host is affected by a privilege escalation vulnerability. |
| Description | The version of VMware Tools installed on the remote Windows host is 11.x prior to 11.2.6. It is, therefore, affected by a local privilege escalation vulnerability. An attacker with normal access to a virtual machine may exploit this issue by placing a malicious file renamed as 'openssl.cnf' in an unrestricted directory which would allow code to be executed with elevated privileges.  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to VMware Tools version 11.2.6 or later. |
| Evidence | Path : C:\Program Files\VMware\VMware Tools\  Installed version : 11.0.1.15528  Fixed version : 11.2.6 |

## Windows Defender Antimalware/Antivirus Signature Definition Check

|  |  |
| --- | --- |
| Criticality | High |
| Synopsis | Windows Defender AntiMalware / AntiVirus Signatures are continuously not and should not be more than 1 day old |
| Description | Windows Defender has an AntiMalware/AntiVirus signature that gets updated continuously. The signature definition has not been updated in more than 1 day. |
| Recommendation | Trigger an update manually and/or enable auto-updates. |
| Evidence | Malware Signature Timestamp : Jul. 17, 2024 at 00:50:31 GMT  Malware Signature Version : 1.415.140.0 |

# Medium Vulnerabilities

## KB5003197: Windows 10 1607 / Windows Server 2016 Security Update (May 2021)

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The remote host is missing one or more security updates. |
| Description | The remote Windows host is missing security updates. It is, therefore, affected by multiple vulnerabilities: Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. |
| Recommendation | Microsoft has released KB5003197 to address this issue. |
| Evidence | The remote host is missing one of the following rollup KBs :   - 5003197   - C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.4283  Should be : 10.0.14393.4402 |

## Windows 10 / Windows Server 2016 September 2017 Information Disclosure Vulnerability (CVE-2017-8529)

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The remote Windows host is affected by an information disclosure vulnerability. |
| Description | The remote Windows host is missing a security update or a registry setting required to enable protections for CVE-2017-8529. It is, therefore, affected by an information disclosure vulnerability:  - An information disclosure vulnerability exists when affected Microsoft scripting engines do not properly handle objects in memory. The vulnerability could allow an attacker to detect specific files on the user's computer. In a web-based attack scenario, an attacker could host a website that is used to attempt to exploit the vulnerability. |
| Recommendation | Refer to the Microsoft CVE article for additional information. |
| Evidence | The following registry key is required to enable the fix for CVE-2017-8529 and is missing.  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_ENABLE\_PRINT\_INFO\_DISCLOSURE\_FIX\iexplore.exe  The following registry key is required to enable the fix for CVE-2017-8529 and is missing.  HKLM\SOFTWARE\WOW6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_ENABLE\_PRINT\_INFO\_DISCLOSURE\_FIX\iexplore.exe |

## Security Updates for Microsoft .NET core (March 2022)

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The Microsoft .NET core installations on the remote host are affected by multiple vulnerabilities. |
| Description | The Microsoft .NET core installations on the remote host are missing security updates. It is, therefore, affected by multiple vulnerabilities:   - A denial of service (DoS) vulnerability. An attacker can exploit this issue to cause the affected component to deny system or application services. (CVE-2022-24464)   - A remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands. (CVE-2020-8927, CVE-2022-24512)  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. |
| Recommendation | Update .NET Core Runtime to version 3.1.23, 5.0.15 or 6.0.3. |
| Evidence | Path : C:\Program Files\dotnet\shared\Microsoft.NetCore.App\3.1.16\  Installed version : 3.1.16.30112  Fixed version : 3.1.23 |

## SMB Signing not required

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | Signing is not required on the remote SMB server. |
| Description | Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server. |
| Recommendation | Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details. |
| Evidence | N/A |

## TLS Version 1.1 Deprecated Protocol

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The remote service encrypts traffic using an older version of TLS. |
| Description | The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1  As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. |
| Recommendation | Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1. |
| Evidence | TLSv1.1 is enabled and the server supports at least one cipher. |

## TLS Version 1.1 Deprecated Protocol

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The remote service encrypts traffic using an older version of TLS. |
| Description | The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1  As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. |
| Recommendation | Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1. |
| Evidence | TLSv1.1 is enabled and the server supports at least one cipher. |

## TLS Version 1.1 Deprecated Protocol

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The remote service encrypts traffic using an older version of TLS. |
| Description | The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1  As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. |
| Recommendation | Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1. |
| Evidence | TLSv1.1 is enabled and the server supports at least one cipher. |

## TLS Version 1.1 Deprecated Protocol

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The remote service encrypts traffic using an older version of TLS. |
| Description | The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1  As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. |
| Recommendation | Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1. |
| Evidence | TLSv1.1 is enabled and the server supports at least one cipher. |

## TLS Version 1.1 Deprecated Protocol

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The remote service encrypts traffic using an older version of TLS. |
| Description | The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1  As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. |
| Recommendation | Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1. |
| Evidence | TLSv1.1 is enabled and the server supports at least one cipher. |

## TLS Version 1.1 Deprecated Protocol

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The remote service encrypts traffic using an older version of TLS. |
| Description | The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1  As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. |
| Recommendation | Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1. |
| Evidence | TLSv1.1 is enabled and the server supports at least one cipher. |

## TLS Version 1.1 Deprecated Protocol

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The remote service encrypts traffic using an older version of TLS. |
| Description | The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1  As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. |
| Recommendation | Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1. |
| Evidence | TLSv1.1 is enabled and the server supports at least one cipher. |

## TLS Version 1.1 Deprecated Protocol

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The remote service encrypts traffic using an older version of TLS. |
| Description | The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1  As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. |
| Recommendation | Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1. |
| Evidence | TLSv1.1 is enabled and the server supports at least one cipher. |

## TLS Version 1.1 Deprecated Protocol

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The remote service encrypts traffic using an older version of TLS. |
| Description | The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1  As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. |
| Recommendation | Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1. |
| Evidence | TLSv1.1 is enabled and the server supports at least one cipher. |

## TLS Version 1.1 Deprecated Protocol

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The remote service encrypts traffic using an older version of TLS. |
| Description | The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1  As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. |
| Recommendation | Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1. |
| Evidence | TLSv1.1 is enabled and the server supports at least one cipher. |

## TLS Version 1.1 Deprecated Protocol

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The remote service encrypts traffic using an older version of TLS. |
| Description | The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1  As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. |
| Recommendation | Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1. |
| Evidence | TLSv1.1 is enabled and the server supports at least one cipher. |

## TLS Version 1.1 Deprecated Protocol

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The remote service encrypts traffic using an older version of TLS. |
| Description | The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1  As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. |
| Recommendation | Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1. |
| Evidence | TLSv1.1 is enabled and the server supports at least one cipher. |

## TLS Version 1.1 Deprecated Protocol

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The remote service encrypts traffic using an older version of TLS. |
| Description | The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1  As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. |
| Recommendation | Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1. |
| Evidence | TLSv1.1 is enabled and the server supports at least one cipher. |

## TLS Version 1.1 Deprecated Protocol

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The remote service encrypts traffic using an older version of TLS. |
| Description | The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1  As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. |
| Recommendation | Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1. |
| Evidence | TLSv1.1 is enabled and the server supports at least one cipher. |

## SSL Self-Signed Certificate

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate chain for this service ends in an unrecognized self-signed certificate. |
| Description | The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.   Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :  |-Subject : CN=HF-SRV-VEEAM-DR.hayleys.net |

## SSL Self-Signed Certificate

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate chain for this service ends in an unrecognized self-signed certificate. |
| Description | The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.   Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :  |-Subject : CN=HF-SRV-VEEAM-DR.hayleys.net |

## SSL Self-Signed Certificate

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate chain for this service ends in an unrecognized self-signed certificate. |
| Description | The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.   Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :  |-Subject : CN=Veeam Backup Server Certificate |

## SSL Self-Signed Certificate

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate chain for this service ends in an unrecognized self-signed certificate. |
| Description | The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.   Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :  |-Subject : CN=Veeam Backup Server Certificate |

## SSL Self-Signed Certificate

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate chain for this service ends in an unrecognized self-signed certificate. |
| Description | The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.   Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :  |-Subject : CN=HF-SRV-VEEAM-DR.hayleys.net |

## SSL Self-Signed Certificate

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate chain for this service ends in an unrecognized self-signed certificate. |
| Description | The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.   Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :  |-Subject : CN=HF-SRV-VEEAM-DR.hayleys.net |

## SSL Self-Signed Certificate

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate chain for this service ends in an unrecognized self-signed certificate. |
| Description | The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.   Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :  |-Subject : OU=Veeam Software/O=Veeam Software/CN=HF-SRV-VEEAM-DR.hayleys.net |

## SSL Self-Signed Certificate

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate chain for this service ends in an unrecognized self-signed certificate. |
| Description | The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.   Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :  |-Subject : CN=Veeam Backup Server Certificate |

## SSL Self-Signed Certificate

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate chain for this service ends in an unrecognized self-signed certificate. |
| Description | The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.   Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :  |-Subject : OU=Veeam Software/O=Veeam Software/CN=HF-SRV-VEEAM-DR.hayleys.net |

## SSL Self-Signed Certificate

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate chain for this service ends in an unrecognized self-signed certificate. |
| Description | The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.   Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :  |-Subject : CN=HF-SRV-VEEAM-DR.hayleys.net |

## SSL Self-Signed Certificate

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate chain for this service ends in an unrecognized self-signed certificate. |
| Description | The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.   Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :  |-Subject : OU=Veeam Software/O=Veeam Software/CN=HF-SRV-VEEAM-DR.hayleys.net |

## SSL Self-Signed Certificate

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate chain for this service ends in an unrecognized self-signed certificate. |
| Description | The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.   Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :  |-Subject : CN=HF-SRV-VEEAM-DR.hayleys.net |

## SSL Self-Signed Certificate

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate chain for this service ends in an unrecognized self-signed certificate. |
| Description | The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.   Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :  |-Subject : OU=Veeam Software/O=Veeam Software/CN=HF-SRV-VEEAM-DR |

## SSL Self-Signed Certificate

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate chain for this service ends in an unrecognized self-signed certificate. |
| Description | The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.   Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :  |-Subject : OU=Veeam Software/O=Veeam Software/CN=HF-SRV-VEEAM-DR.hayleys.net |

## SSL Self-Signed Certificate

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate chain for this service ends in an unrecognized self-signed certificate. |
| Description | The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.   Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :  |-Subject : CN=Veeam Backup Server Certificate |

## SSL Certificate Cannot Be Trusted

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate for this service cannot be trusted. |
| Description | The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :   - First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.   - Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.   - Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.  If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :  |-Subject : CN=HF-SRV-VEEAM-DR.hayleys.net |-Issuer : CN=HF-SRV-VEEAM-DR.hayleys.net |

## SSL Certificate Cannot Be Trusted

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate for this service cannot be trusted. |
| Description | The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :   - First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.   - Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.   - Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.  If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :  |-Subject : CN=HF-SRV-VEEAM-DR.hayleys.net |-Issuer : CN=HF-SRV-VEEAM-DR.hayleys.net |

## SSL Certificate Cannot Be Trusted

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate for this service cannot be trusted. |
| Description | The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :   - First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.   - Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.   - Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.  If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :  |-Subject : CN=Veeam Backup Server Certificate |-Issuer : CN=Veeam Backup Server Certificate |

## SSL Certificate Cannot Be Trusted

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate for this service cannot be trusted. |
| Description | The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :   - First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.   - Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.   - Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.  If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :  |-Subject : CN=Veeam Backup Server Certificate |-Issuer : CN=Veeam Backup Server Certificate |

## SSL Certificate Cannot Be Trusted

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate for this service cannot be trusted. |
| Description | The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :   - First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.   - Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.   - Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.  If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :  |-Subject : CN=HF-SRV-VEEAM-DR.hayleys.net |-Issuer : CN=HF-SRV-VEEAM-DR.hayleys.net |

## SSL Certificate Cannot Be Trusted

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate for this service cannot be trusted. |
| Description | The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :   - First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.   - Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.   - Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.  If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :  |-Subject : CN=HF-SRV-VEEAM-DR.hayleys.net |-Issuer : CN=HF-SRV-VEEAM-DR.hayleys.net |

## SSL Certificate Cannot Be Trusted

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate for this service cannot be trusted. |
| Description | The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :   - First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.   - Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.   - Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.  If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :  |-Subject : OU=Veeam Software/O=Veeam Software/CN=HF-SRV-VEEAM-DR.hayleys.net |-Issuer : OU=Veeam Software/O=Veeam Software/CN=HF-SRV-VEEAM-DR.hayleys.net |

## SSL Certificate Cannot Be Trusted

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate for this service cannot be trusted. |
| Description | The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :   - First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.   - Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.   - Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.  If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :  |-Subject : CN=Veeam Backup Server Certificate |-Issuer : CN=Veeam Backup Server Certificate |

## SSL Certificate Cannot Be Trusted

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate for this service cannot be trusted. |
| Description | The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :   - First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.   - Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.   - Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.  If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :  |-Subject : OU=Veeam Software/O=Veeam Software/CN=HF-SRV-VEEAM-DR.hayleys.net |-Issuer : OU=Veeam Software/O=Veeam Software/CN=HF-SRV-VEEAM-DR.hayleys.net |

## SSL Certificate Cannot Be Trusted

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate for this service cannot be trusted. |
| Description | The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :   - First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.   - Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.   - Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.  If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :  |-Subject : CN=HF-SRV-VEEAM-DR.hayleys.net |-Issuer : CN=HF-SRV-VEEAM-DR.hayleys.net |

## SSL Certificate Cannot Be Trusted

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate for this service cannot be trusted. |
| Description | The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :   - First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.   - Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.   - Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.  If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :  |-Subject : OU=Veeam Software/O=Veeam Software/CN=HF-SRV-VEEAM-DR.hayleys.net |-Issuer : OU=Veeam Software/O=Veeam Software/CN=HF-SRV-VEEAM-DR.hayleys.net |

## SSL Certificate Cannot Be Trusted

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate for this service cannot be trusted. |
| Description | The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :   - First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.   - Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.   - Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.  If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :  |-Subject : CN=HF-SRV-VEEAM-DR.hayleys.net |-Issuer : CN=HF-SRV-VEEAM-DR.hayleys.net |

## SSL Certificate Cannot Be Trusted

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate for this service cannot be trusted. |
| Description | The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :   - First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.   - Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.   - Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.  If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :  |-Subject : OU=Veeam Software/O=Veeam Software/CN=HF-SRV-VEEAM-DR |-Issuer : OU=Veeam Software/O=Veeam Software/CN=HF-SRV-VEEAM-DR |

## SSL Certificate Cannot Be Trusted

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate for this service cannot be trusted. |
| Description | The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :   - First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.   - Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.   - Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.  If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :  |-Subject : OU=Veeam Software/O=Veeam Software/CN=HF-SRV-VEEAM-DR.hayleys.net |-Issuer : OU=Veeam Software/O=Veeam Software/CN=HF-SRV-VEEAM-DR.hayleys.net |

## SSL Certificate Cannot Be Trusted

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate for this service cannot be trusted. |
| Description | The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :   - First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.   - Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.   - Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.  If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :  |-Subject : CN=Veeam Backup Server Certificate |-Issuer : CN=Veeam Backup Server Certificate |

## SSL Certificate with Wrong Hostname

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate for this service is for a different host. |
| Description | The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The identities known by Nessus are :   10.40.21.241  hf-srv-veeam-dr  10.40.21.241  The Common Name in the certificate is :   HF-SRV-VEEAM-DR.hayleys.net  The Subject Alternate Name in the certificate is :   HF-SRV-VEEAM-DR.hayleys.net |

## SSL Certificate with Wrong Hostname

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate for this service is for a different host. |
| Description | The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The identities known by Nessus are :   10.40.21.241  hf-srv-veeam-dr  10.40.21.241  The Common Name in the certificate is :   HF-SRV-VEEAM-DR.hayleys.net |

## SSL Certificate with Wrong Hostname

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate for this service is for a different host. |
| Description | The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The identities known by Nessus are :   10.40.21.241  hf-srv-veeam-dr  10.40.21.241  The Common Name in the certificate is :   Veeam Backup Server Certificate |

## SSL Certificate with Wrong Hostname

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate for this service is for a different host. |
| Description | The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The identities known by Nessus are :   10.40.21.241  hf-srv-veeam-dr  10.40.21.241  The Common Name in the certificate is :   Veeam Backup Server Certificate |

## SSL Certificate with Wrong Hostname

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate for this service is for a different host. |
| Description | The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The identities known by Nessus are :   10.40.21.241  hf-srv-veeam-dr  10.40.21.241  The Common Name in the certificate is :   HF-SRV-VEEAM-DR.hayleys.net  The Subject Alternate Name in the certificate is :   HF-SRV-VEEAM-DR.hayleys.net |

## SSL Certificate with Wrong Hostname

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate for this service is for a different host. |
| Description | The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The identities known by Nessus are :   10.40.21.241  hf-srv-veeam-dr  10.40.21.241  The Common Name in the certificate is :   HF-SRV-VEEAM-DR.hayleys.net  The Subject Alternate Name in the certificate is :   HF-SRV-VEEAM-DR.hayleys.net |

## SSL Certificate with Wrong Hostname

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate for this service is for a different host. |
| Description | The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The identities known by Nessus are :   10.40.21.241  hf-srv-veeam-dr  10.40.21.241  The Common Name in the certificate is :   HF-SRV-VEEAM-DR.hayleys.net  The Subject Alternate Name in the certificate is :   HF-SRV-VEEAM-DR.hayleys.net |

## SSL Certificate with Wrong Hostname

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate for this service is for a different host. |
| Description | The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The identities known by Nessus are :   10.40.21.241  hf-srv-veeam-dr  10.40.21.241  The Common Name in the certificate is :   Veeam Backup Server Certificate |

## SSL Certificate with Wrong Hostname

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate for this service is for a different host. |
| Description | The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The identities known by Nessus are :   10.40.21.241  hf-srv-veeam-dr  10.40.21.241  The Common Name in the certificate is :   HF-SRV-VEEAM-DR.hayleys.net  The Subject Alternate Name in the certificate is :   HF-SRV-VEEAM-DR.hayleys.net |

## SSL Certificate with Wrong Hostname

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate for this service is for a different host. |
| Description | The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The identities known by Nessus are :   10.40.21.241  hf-srv-veeam-dr  10.40.21.241  The Common Name in the certificate is :   HF-SRV-VEEAM-DR.hayleys.net  The Subject Alternate Name in the certificate is :   HF-SRV-VEEAM-DR.hayleys.net |

## SSL Certificate with Wrong Hostname

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate for this service is for a different host. |
| Description | The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The identities known by Nessus are :   10.40.21.241  hf-srv-veeam-dr  10.40.21.241  The Common Name in the certificate is :   HF-SRV-VEEAM-DR.hayleys.net  The Subject Alternate Name in the certificate is :   HF-SRV-VEEAM-DR.hayleys.net |

## SSL Certificate with Wrong Hostname

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate for this service is for a different host. |
| Description | The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The identities known by Nessus are :   10.40.21.241  hf-srv-veeam-dr  10.40.21.241  The Common Name in the certificate is :   HF-SRV-VEEAM-DR.hayleys.net  The Subject Alternate Name in the certificate is :   HF-SRV-VEEAM-DR.hayleys.net |

## SSL Certificate with Wrong Hostname

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate for this service is for a different host. |
| Description | The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The identities known by Nessus are :   10.40.21.241  hf-srv-veeam-dr  10.40.21.241  The Common Name in the certificate is :   HF-SRV-VEEAM-DR.hayleys.net  The Subject Alternate Name in the certificate is :   HF-SRV-VEEAM-DR.hayleys.net |

## SSL Certificate with Wrong Hostname

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The SSL certificate for this service is for a different host. |
| Description | The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine. |
| Recommendation | Purchase or generate a proper SSL certificate for this service. |
| Evidence | The identities known by Nessus are :   10.40.21.241  hf-srv-veeam-dr  10.40.21.241  The Common Name in the certificate is :   Veeam Backup Server Certificate |

## Google Chrome < 129.0.6668.58 Multiple Vulnerabilities

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | A web browser installed on the remote Windows host is affected by multiple vulnerabilities. |
| Description | The version of Google Chrome installed on the remote Windows host is prior to 129.0.6668.58. It is, therefore, affected by multiple vulnerabilities as referenced in the 2024\_09\_stable-channel-update-for-desktop\_17 advisory.   - Type Confusion in V8. (CVE-2024-8904)   - Inappropriate implementation in V8. (CVE-2024-8905)   - Incorrect security UI in Downloads. (CVE-2024-8906)   - Insufficient data validation in Omnibox. (CVE-2024-8907)   - Inappropriate implementation in Autofill. (CVE-2024-8908)   - Inappropriate implementation in UI. (CVE-2024-8909)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to Google Chrome version 129.0.6668.58 or later. |
| Evidence | Path : C:\Program Files\Google\Chrome\Application  Installed version : 126.0.6478.128  Fixed version : 129.0.6668.58 |

## WinSCP < 6.3.3 Key Recovery Attack Vulnerability

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | A file transfer application installed on the remote Windows host is affected by a key recovery attack vulnerability. |
| Description | The version of WinSCP installed on the remote Windows host is prior to 6.3.3. It is, therefore, affected by a key recovery attack vulnerability. In PuTTY 0.68 through 0.80 before 0.81, biased ECDSA nonce generation allows an attacker to recover a user's NIST P-521 secret key via a quick attack in approximately 60 signatures. This is especially important in a scenario where an adversary is able to read messages signed by PuTTY or Pageant. The required set of signed messages may be publicly readable because they are stored in a public Git service that supports use of SSH for commit signing, and the signatures were made by Pageant through an agent-forwarding mechanism. In other words, an adversary may already have enough signature information to compromise a victim's private key, even if there is no further use of vulnerable PuTTY versions. After a key compromise, an adversary may be able to conduct supply-chain attacks on software maintained in Git. A second, independent scenario is that the adversary is an operator of an SSH server to which the victim authenticates (for remote login or file copy), even though this server is not fully trusted by the victim, and the victim uses the same private key for SSH connections to other services operated by other entities. Here, the rogue server operator (who would otherwise have no way to determine the victim's private key) can derive the victim's private key, and then use it for unauthorized access to those other services. If the other services include Git services, then again it may be possible to conduct supply-chain attacks on software maintained in Git. This also affects, for example, FileZilla before 3.67.0, WinSCP before 6.3.3, TortoiseGit before 2.15.0.1, and TortoiseSVN through 1.14.6.  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to WinSCP version 6.3.3 or later. |
| Evidence | Path : C:\Program Files (x86)\WinSCP\  Installed version : 5.15.1.9407  Fixed version : 6.3.3 |

## Security Updates for Windows Malicious Software Removal Tool (January 2023)

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The remote Windows host has an antimalware application that is affected by a privilege escalation vulnerability. |
| Description | The Windows Malicious Software Removal Tool installation on the remote host is missing a security update. It is, therefore, affected by the following vulnerability:    - An elevation of privilege vulnerability. An attacker can exploit this to gain elevated privileges.  (CVE-2023-21725) |
| Recommendation | Microsoft has released version 5.109 to address this issue. |
| Evidence | Product : Microsoft Malicious Software Removal Tool  Installed version : 5.87.17921.1  Fixed version : 5.109.19957.1 |

## VMware Tools 10.x / 11.x / 12.x < 12.1.5 DoS (VMSA-2022-0029)

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | A virtualization tool suite is installed on the remote Windows host is affected by a denial of service vulnerability. |
| Description | The version of VMware Tools installed on the remote Windows host is affected by a denial of service vulnerability in the VM3DMP driver. An authenticated, local attacker can exploit this to trigger a PANIC in the VM3DMP driver leading to a denial-of-service condition in the Windows guest OS.  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to VMware Tools version 12.1.5 or later. |
| Evidence | Path : C:\Program Files\VMware\VMware Tools\  Installed version : 11.0.1.15528  Fixed version : 12.1.5 |

## Security Updates for Microsoft .NET Core (August 2022)

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The Microsoft .NET core installations on the remote host are affected by a spoofing vulnerability. |
| Description | A spoofing vulnerability exists in .NET core 6.0 < 6.0.8 and .NET Core 3.1 < 3.1.28. An unauthenticated, remote attacker can exploit this, to perform actions with the privileges of another user.  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. |
| Recommendation | Update .NET Core Runtime to version 3.1.28 or 6.0.8. |
| Evidence | Path : C:\Program Files\dotnet\shared\Microsoft.NetCore.App\3.1.16\  Installed version : 3.1.16.30112  Fixed version : 3.1.28 |

## Security Updates for Microsoft .NET core (June 2022)

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The Microsoft .NET core installations on the remote host are affected by an information disclosure vulnerability. |
| Description | An information disclosure vulnerability exists in .NET core 6.0 < 6.0.6 and .NET Core 3.1 < 3.1.26. An unauthenticated, local attacker can exploit this, to disclose potentially sensitive information.  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. |
| Recommendation | Update .NET Core Runtime to version 3.1.26 or 6.0.6. |
| Evidence | Path : C:\Program Files\dotnet\shared\Microsoft.NetCore.App\3.1.16\  Installed version : 3.1.16.30112  Fixed version : 3.1.26 |

## Security Update for Microsoft ASP.NET Core (August 2021)

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The Microsoft ASP.NET Core installations on the remote host is affected by multiple vulnerabilities. |
| Description | The Microsoft ASP.NET Core installation on the remote host is version 2.1.x prior to 2.1.29, 3.1.x prior to 3.1.18, or 5.x prior to 5.0.9. It is, therefore, affected by multiple vulnerabilities:   - A denial of service (DoS) vulnerability. An attacker can exploit this issue to cause the affected component to deny system or application services. (CVE-2021-26423)   - An information disclosure vulnerability. An attacker can exploit this to disclose potentially sensitive information. (CVE-2021-34485, CVE-2021-34532)  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. |
| Recommendation | Update ASP.NET Core, remove vulnerable packages and refer to vendor advisory. |
| Evidence | Path : C:\Program Files\dotnet\shared\Microsoft.AspNetCore.App\3.1.16  Installed version : 3.1.16  Fixed version : 3.1.18 |

## VMware Tools 11.x < 11.3.0 DoS (VMSA-2021-0011)

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | A virtualization tool suite is installed on the remote Windows host is affected by a denial-of-service vulnerability. |
| Description | The version of VMware Tools installed on the remote Windows host is 11.x, which is prior to 11.3.0. It is, therefore, affected by a denial-of-service vulnerability in the VM3DMP driver. A malicious actor with local user privileges in the Windows guest operating system, where VMware Tools is installed, can trigger a PANIC in the VM3DMP driver leading to a denial-of-service condition in the Windows guest operating system.  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to VMware Tools version 11.3.0 or later. |
| Evidence | Path : C:\Program Files\VMware\VMware Tools\  Installed version : 11.0.1.15528  Fixed version : 11.3.0 |

## Windows Speculative Execution Configuration Check

|  |  |
| --- | --- |
| Criticality | Medium |
| Synopsis | The remote host has not properly mitigated a series of speculative execution vulnerabilities. |
| Description | The remote host has not properly mitigated a series of known speculative execution vulnerabilities. It, therefore, may be affected by :  - Branch Target Injection (BTI) (CVE-2017-5715)  - Bounds Check Bypass (BCB) (CVE-2017-5753)  - Rogue Data Cache Load (RDCL) (CVE-2017-5754)  - Rogue System Register Read (RSRE) (CVE-2018-3640)  - Speculative Store Bypass (SSB) (CVE-2018-3639)  - L1 Terminal Fault (L1TF) (CVE-2018-3615, CVE-2018-3620, CVE-2018-3646)  - Microarchitectural Data Sampling Uncacheable Memory (MDSUM) (CVE-2019-11091)  - Microarchitectural Store Buffer Data Sampling (MSBDS) (CVE-2018-12126)  - Microarchitectural Load Port Data Sampling (MLPDS) (CVE-2018-12127)  - Microarchitectural Fill Buffer Data Sampling (MFBDS) (CVE-2018-12130)  - TSX Asynchronous Abort (TAA) (CVE-2019-11135) |
| Recommendation | Apply vendor recommended settings. |
| Evidence | Current Settings:  - SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\  FeatureSettingsOverrideMask: Not Set  - SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\  FeatureSettingsOverride: Not Set  -----------------------------------  Recommended Settings 1:  - SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\  FeatureSettingsOverrideMask: 0x00000003 (3)  - SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\  FeatureSettingsOverride: 0x00000048 (72)  CVEs Covered:  CVE-2017-5715, CVE-2017-5753, CVE-2017-5754, CVE-2018-3615, CVE-2018-3620,  CVE-2018-3639, CVE-2018-3646, CVE-2018-11091, CVE-2018-12126, CVE-2018-12127,  CVE-2018-12130, CVE-2019-11135  Note: Hyper-Threading enabled.  -----------------------------------  Recommended Settings 2:  - SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\  FeatureSettingsOverrideMask: 0x00000003 (3)  - SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\  FeatureSettingsOverride: 0x00002048 (8264)  CVEs Covered:  CVE-2017-5715, CVE-2017-5753, CVE-2017-5754, CVE-2018-3615, CVE-2018-3620,  CVE-2018-3639, CVE-2018-3646, CVE-2018-11091, CVE-2018-12126, CVE-2018-12127,  CVE-2018-12130, CVE-2019-11135  Note: Hyper-Threading disabled. |

# Low Vulnerabilities

## ICMP Timestamp Request Remote Date Disclosure

|  |  |
| --- | --- |
| Criticality | Low |
| Synopsis | It is possible to determine the exact time set on the remote host. |
| Description | The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.  Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time. |
| Recommendation | Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14). |
| Evidence | This host returns non-standard timestamps (high bit is set) The ICMP timestamps might be in little endian format (not in network format) The difference between the local and remote clocks is 14 seconds. |

## VMware Tools 10.3.x / 11.x / 12.x < 12.2.5 Authentication Bypass (VMSA-2023-0013)

|  |  |
| --- | --- |
| Criticality | Low |
| Synopsis | The virtualization tool suite is installed on the remote Windows host is affected by an authentication bypass vulnerability. |
| Description | The version of VMware Tools installed on the remote Windows host is affected by an authentication bypass vulnerability in the vgauth module. A fully compromised ESXi host can force VMware Tools to fail to authenticate host-to-guest operations, impacting the confidentiality and integrity of the guest virtual machine.  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. |
| Recommendation | Upgrade to VMware Tools version 12.2.5 or later. |
| Evidence | Path : C:\Program Files\VMware\VMware Tools\  Installed version : 11.0.1.15528  Fixed version : 12.2.5 |