

High (CVSS: 10.0)

NVT: Microsoft Windows Multiple Vulnerabilities (KB5025279)

**Summary**

This host is missing an important security update according to Microsoft KB5025279

**Vulnerability Detection Result** Vulnerable range: Less than 6.1.7601.26465 File checked: C:\Windows\system32\Ntoskrnl.exe File version: 6.1.7600.16385

**Impact**

Successful exploitation will allow an attacker to elevate privileges, execute arbitrary commands, disclose information and conduct DoS attacks.

**Solution**

**Solution type:** VendorFix

The vendor has released updates. Please see the references for more information.

**Affected Software/OS**

Microsoft Windows Server 2008 R2 for x64-based Systems Service Pack 1.

**Vulnerability Insight** Multiple flaws exist due to: - An Elevation of Privilege Vulnerability in Windows Kernel. - An Elevation of Privilege Vulnerability in Windows Ancillary Function Driver for WinSock. - A Remote Code Execution Vulnerability in Microsoft Message Queuing. For more information about the vulnerabilities refer to Reference links.

**Vulnerability Detection Method** Checks if a vulnerable version is present on the target host. Details: Microsoft Windows Multiple Vulnerabilities (KB5025279) (OID: 1.3.6.1.4.1.25623.1.0.832037) Version used: 2023-05-18T09:08:59Z

**References**

CVE-2023-21729,CVE-2023-28308,CVE-2023-28307,CVE-2023-28306,CVE-2023-28305,CVE-2023-28302,CVE-2023-28298,CVE-2023-28293,CVE-2023-28256,CVE-2023-28278,CVE-2023-28255,CVE-2023-28253,CVE-2023-28254,CVE-2023-28276,CVE-2023-28275,CVE-2023-28252,CVE-2023-28250,CVE-2023-28272,CVE-2023-28271,CVE-2023-28268,CVE-2023-28244,CVE-2023-28266,CVE-2023-28267,CVE-2023-28241,CVE-2023-28240,CVE-2023-28238,CVE-2023-28232,CVE-2023-28231,CVE-2023-28228,CVE-2023-28229,CVE-2023-28227,CVE-2023-28223,CVE-2023-28222,CVE-2023-28220,CVE-2023-28219,CVE-2023-28218,CVE-2023-28217,CVE-2023-28216,CVE-2023-24931,CVE-2023-24912,CVE-2023-21769,CVE-2023-21727,CVE-2023-21554

High (CVSS: 10.0)

NVT: Microsoft Windows HTTP.sys Remote Code Execution Vulnerability (3042553)

**Summary**

This host is missing an important security update according to Microsoft Bulletin MS15-034.

**Vulnerability Detection Result** The target host was found to be vulnerable

**Impact**

Successful exploitation will allow remote attackers to run arbitrary code in the context of the current user and to perform actions in the security context of the current user.

**Solution**

**Solution type:** VendorFix

The vendor has released updates. Please see the references for more information.

**Affected Software/OS**

''- Microsoft Windows 8 x32/x64

**Vulnerability Insight**

**Vulnerability Detection Method**

**References**  
CVE-2015-1635