



CVE-2016-7224

Published on: 11/10/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:06 PM UTC

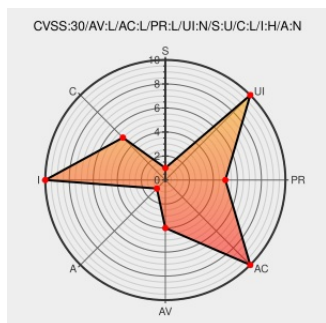
CVE-2016-7224

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



Certain versions of [Windows 10](#) from [Microsoft](#) contain the following vulnerability:

Virtual Hard Disk Driver in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 does not properly restrict access to files, which allows local users to gain privileges via a crafted application, aka "VHD Driver Elevation of Privilege Vulnerability."

CVE-2016-7224 has been assigned by [secure@microsoft.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector

Attack Complexity

Privileges Required

User Interaction

LOCAL

LOW

LOW

NONE

Scope

Confidentiality Impact

Integrity Impact

Availability Impact

UNCHANGED

LOW

HIGH

NONE

CVSS2 Score: **3.6 - LOW**

Access Vector

Access Complexity

Authentication

LOCAL

LOW

NONE

Confidentiality Impact

Integrity Impact

Availability Impact

PARTIAL

PARTIAL

NONE

CVE References

Description

Tags

Link

Microsoft Security Bulletin MS16-138 - Important | Microsoft Docs

[docs.microsoft.com](#)
[text/html](#)

MS MS16-138

Microsoft Windows - VHDMP Arbitrary Physical Disk Cloning Privilege Escalation (MS16-138) -

[www.exploit-db.com](#)

EXPLOIT-

Microsoft Windows - Virtual Hard Disk Driver Lets Local Users Modify Restricted Files to Gain Elevated Privileges - Exploit-DB	www.exploit-db.com Proof of Concept text/html	 Exploit-DB DB 40765
Microsoft Virtual Hard Disk Driver Lets Local Users Modify Restricted Files to Gain Elevated Privileges - SecurityTracker	www.securitytracker.com text/html	 SECTRAK 1037248
Microsoft Windows CVE-2016-7224 Local Privilege Escalation Vulnerability	cve.report (archive) text/html	 BID 94017

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 10	-	All	All	All
Operating System	Microsoft	Windows 10	1511	All	All	All
Operating System	Microsoft	Windows 10	1607	All	All	All
Operating System	Microsoft	Windows 10	-	All	All	All
Operating System	Microsoft	Windows 10	1511	All	All	All
Operating System	Microsoft	Windows 10	1607	All	All	All
Operating System	Microsoft	Windows 8.1	All	All	All	All
Operating System	Microsoft	Windows 8.1	All	All	All	All
Operating System	Microsoft	Windows Rt 8.1	All	All	All	All
Operating System	Microsoft	Windows Rt 8.1	All	All	All	All
Operating System	Microsoft	Windows Server 2012	-	All	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Server 2012	-	All	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Server 2016	-	All	All	All

System						
Operating System	Microsoft	Windows Server 2016	-	All	All	All
cpe:2.3:o:microsoft:windows_10:-:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_10:1511:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_10:1607:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_10:-:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_10:1511:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_10:1607:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_8.1:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_8.1:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_rt_8.1:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_rt_8.1:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_server_2012:-:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_server_2012:r2:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_server_2012:-:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_server_2012:r2:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_server_2016:-:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_server_2016:-:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)