



CVE-2016-3216

Published on: 06/15/2016 12:00:00 AM UTC

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

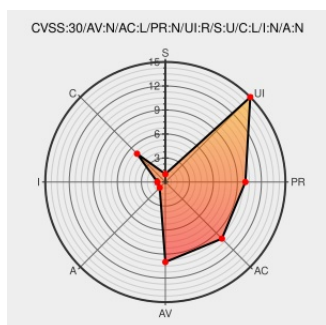
CVE-2016-3216

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

GDI32.dll in the Graphics component in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to bypass the ASLR protection mechanism via unspecified vectors, aka "Windows Graphics Component Information Disclosure Vulnerability."

CVE-2016-3216 has been assigned by secure@microsoft.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **4.3 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	LOW	NONE	NONE

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Microsoft Graphics Component Bugs Lets Local Users Bypass ASLR Protection and Gain Elevated Privileges - SecurityTracker	www.securitytracker.com text/html	SECTRACK

Microsoft Security Bulletin MS16-074 - Important | Microsoft Docs

docs.microsoft.com[text/html](#) MS
MS16-074

Microsoft Windows - 'gdi32.dll' Multiple DIB-Related EMF Record Handlers Heap Out-of-Bounds Reads/Memory Disclosure (MS16-074) - Windows dos Exploit

www.exploit-db.com[Proof of Concept](#)[text/html](#) EXPLOIT-
DB 39990

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	-	All	All	All
Operating System	Microsoft	Windows 10	1511	All	All	All
Operating System	Microsoft	Windows 7	All	All	All	All
Operating System	Microsoft	Windows 7	All	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 2008	All	sp2	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2008	All	sp2	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	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 Vista	All	sp2	All	All
Operating System	Microsoft	Windows Vista	All	sp2	All	All
cpe:2.3:o:microsoft:windows_10:-:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_10:1511:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_10:-:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_10:1511:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_7:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_7:*:*:*:*:*:						
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_2008:*:sp2:*:*:*:*:						
cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:*:						
cpe:2.3:o:microsoft:windows_server_2008:*:sp2:*:*:*:*:						
cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:*:						
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_vista:*:sp2:*:*:*:*:						
cpe:2.3:o:microsoft:windows_vista:*:sp2:*:*:*:*:						

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)