

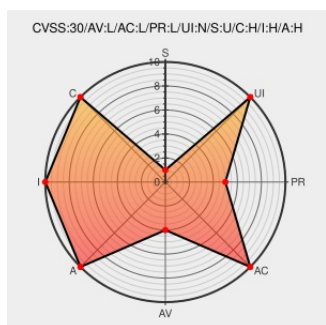


CVE-2016-7185

Published on: 10/13/2016 12:00:00 AM UTC

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

CVE-2016-7185

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

The kernel-mode drivers 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, 1511, and 1607 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability." a different vulnerability than CVE-2016-3266, CVE-2016-3376, and CVE-2016-7211.

CVE-2016-7185 has been assigned by secure@microsoft.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.2 - HIGH**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Microsoft Windows Kernel 'Win32k.sys' CVE-2016-7185 Local Privilege Escalation Vulnerability	cve.report (archive) text/html	BID 93389

Microsoft Security Bulletin MS16-123 - Important Microsoft Docs	docs.microsoft.com text/html	 MS MS16-123
Microsoft Windows - DFS Client Driver Arbitrary Drive Mapping Privilege Escalation (MS16-123) - Windows local Exploit	www.exploit-db.com Proof of Concept text/html	 EXPLOIT-DB 40572
Windows Kernel-Mode Drivers Lets Local Users Gain Elevated Privileges - SecurityTracker	www.securitytracker.com text/html	 SECTRAK 1036996

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 7	All	sp1	All	All
Operating System	Microsoft	Windows 7	All	sp1	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

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

← Previous ID

Next ID→