



CVE-2015-1722

Published on: 06/09/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:10 PM UTC

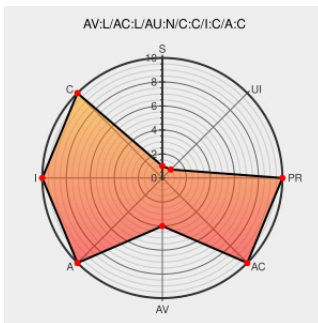
CVE-2015-1722

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Windows 7](#) from [Microsoft](#) contain the following vulnerability:

Use-after-free vulnerability in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka "Microsoft Windows Kernel Bitmap Handling Use After Free Vulnerability."

CVE-2015-1722 has been assigned by secure@microsoft.com to track the vulnerability

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 - Bitmap Handling Use-After-Free (MS15-061) (2) - Windows_x86 dos Exploit	Exploit Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 38265
Microsoft Security Bulletin MS15-061 - Important Microsoft Docs	Patch Vendor Advisory docs.microsoft.com text/html	MS MS15-061
Microsoft Windows Kernel - Bitmap Handling Use-After-Free (MS15-061) (1) - Windows_x86 dos Exploit	Exploit Third Party Advisory	EXPLOIT-DB 38275

EXPLOIT

Third Party Advisory

VDB Entry

www.exploit-db.com

Proof of Concept

text/html

DB 56273

Windows Kernel Lets Local Users Obtain Potentially Sensitive Information and Gain Elevated Privileges - SecurityTracker

Third Party Advisory

VDB Entry

www.securitytracker.com

text/html

SECTrack
1032525

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 7	-	sp1	All	All
Operating System	Microsoft	Windows 7	-	sp1	All	All
Operating System	Microsoft	Windows 8	-	All	All	All
Operating System	Microsoft	Windows 8	-	All	All	All
Operating System	Microsoft	Windows 8.1	-	All	All	All
Operating System	Microsoft	Windows 8.1	-	All	All	All
Operating System	Microsoft	Windows Rt	-	All	All	All
Operating System	Microsoft	Windows Rt	-	All	All	All
Operating System	Microsoft	Windows Rt 8.1	-	All	All	All
Operating System	Microsoft	Windows Rt 8.1	-	All	All	All
Operating System	Microsoft	Windows Server 2003	-	sp2	All	All
Operating System	Microsoft	Windows Server 2003	r2	sp2	All	All
Operating System	Microsoft	Windows Server 2003	-	sp2	All	All
Operating System	Microsoft	Windows Server 2003	r2	sp2	All	All
Operating System	Microsoft	Windows Server 2008	-	sp2	All	All

System						
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2008	-	sp2	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	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	-	sp2	All	All
Operating System	Microsoft	Windows Vista	-	sp2	All	All
cpe:2.3:o:microsoft:windows_7:-:sp1:*****:.*:						
cpe:2.3:o:microsoft:windows_7:-:sp1:*****:.*:						
cpe:2.3:o:microsoft:windows_8:-:*****:.*:						
cpe:2.3:o:microsoft:windows_8:-:*****:.*:						
cpe:2.3:o:microsoft:windows_8.1:-:*****:.*:						
cpe:2.3:o:microsoft:windows_8.1:-:*****:.*:						
cpe:2.3:o:microsoft:windows_rt:-:*****:.*:						
cpe:2.3:o:microsoft:windows_rt:-:*****:.*:						
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_2003:-:sp2:*****:.*:						
cpe:2.3:o:microsoft:windows_server_2003:r2:sp2:*****:.*:						
cpe:2.3:o:microsoft:windows_server_2003:-:sp2:*****:.*:						
cpe:2.3:o:microsoft:windows_server_2003:r2:sp2:*****:.*:						

cpe:2.3:o:microsoft:windows_server_2008:-:sp2:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:*:itanium:*:
cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:*:x64:*:
cpe:2.3:o:microsoft:windows_server_2008:-:sp2:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:*:itanium:*:
cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:*:x64:*:
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

[← Previous ID](#)

Next ID→

© 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