



CVE-2015-1671

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2015-1671
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-05-13 10:59:00 UTC
Updated	2018-10-12 22:08:00 UTC
Description	The Windows DirectWrite library, as used in Microsoft .NET Framework 3.0 SP2, 3.5, 3.5.1, 4, 4.5, 4.5.1, and 4.5.2; Office 2

Risk And Classification

EPSS: 0.859280000 probability, percentile 0.993890000 (date 2026-04-14)

CISA KEV: Listed on 2022-05-25; due 2022-06-15; ransomware use Unknown

Problem Types: CWE-19

CISA Known Exploited Vulnerability

Vendor	Microsoft
Product	Windows
Name	Microsoft Windows Remote Code Execution Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2015-1671

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	.net Framework	3.0	sp2	All	All
Application	Microsoft	.net Framework	3.5	All	All	All
Application	Microsoft	.net Framework	3.5.1	All	All	All
Application	Microsoft	.net Framework	4.0	All	All	All
Application	Microsoft	.net Framework	4.5	All	All	All
Application	Microsoft	.net Framework	4.5.1	All	All	All
Application	Microsoft	.net Framework	4.5.2	All	All	All
Application	Microsoft	.net Framework	3.0	sp2	All	All

Application	Microsoft	.net Framework	3.5	All	All	All
Application	Microsoft	.net Framework	3.5.1	All	All	All
Application	Microsoft	.net Framework	4.0	All	All	All
Application	Microsoft	.net Framework	4.5	All	All	All
Application	Microsoft	.net Framework	4.5.1	All	All	All
Application	Microsoft	.net Framework	4.5.2	All	All	All
Application	Microsoft	Live Meeting	2007	All	All	All
Application	Microsoft	Live Meeting	2007	All	All	All
Application	Microsoft	Lync	2010	All	All	All
Application	Microsoft	Lync	2010	All	All	All
Application	Microsoft	Lync	2010	All	All	All
Application	Microsoft	Lync	2013	sp1	All	All
Application	Microsoft	Lync	2013	sp1	All	All
Application	Microsoft	Lync	2010	All	All	All
Application	Microsoft	Lync	2010	All	All	All
Application	Microsoft	Lync	2010	All	All	All
Application	Microsoft	Lync	2013	sp1	All	All
Application	Microsoft	Lync	2013	sp1	All	All
Application	Microsoft	Office	2007	sp3	All	All
Application	Microsoft	Office	2010	sp2	All	All
Application	Microsoft	Office	2010	sp2	All	All
Application	Microsoft	Office	2007	sp3	All	All
Application	Microsoft	Office	2010	sp2	All	All
Application	Microsoft	Office	2010	sp2	All	All
Application	Microsoft	Silverlight	All	developer_runtime	All	All
Application	Microsoft	Silverlight	All	All	All	All

References

Reference

Microsoft Windows OpenType and TrueType Font Parsing Errors Let Remote Users Execute Arbitrary Code and Obtain Potentially Sensitive I

Microsoft Security Bulletin MS15-044 - Critical | Microsoft Docs

Microsoft Windows GDI+ CVE-2015-1671 TrueType Font Handling Remote Code Execution Vulnerability

CVE Program record

NVD vulnerability detail

CISA Known Exploited Vulnerabilities catalog

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

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