



CVE-2014-4071

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2014-4071
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-09-10 01:55:00 UTC
Updated	2018-10-12 22:06:00 UTC
Description	The Server in Microsoft Lync Server 2013 allows remote attackers to cause a denial of service (NULL pointer dereference and

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Lync Server	2013	All	All	All
Application	Microsoft	Lync Server	2013	All	All	All

References

Reference	Source	Link
Microsoft Security Bulletin MS14-055 - Important Microsoft Docs	MS	docs.m
Microsoft Lync Server CVE-2014-4071 Remote Denial of Service Vulnerability	BID	www.s
Microsoft Lync Bugs Permit Cross-Site Scripting and Denial of Service Attacks - SecurityTracker	SECTRACK	www.s
IBM X-Force Exchange	XF	exchar
Assessing risk for the September 2014 security updates - Security Research & Defense - Site Home - TechNet Blogs	CONFIRM	blogs.t
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.nis

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](#)