



CVE-2015-2532

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2015-2532
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-09-09 00:59:00 UTC
Updated	2018-10-12 22:09:00 UTC
Description	Cross-site scripting (XSS) vulnerability in Microsoft Lync Server 2013 allows remote attackers to inject arbitrary web script c

Risk And Classification

Problem Types: CWE-79

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 Lync Input Validation Flaws Let Remote Conduct Cross-Site Scripting Attacks - SecurityTracker	SECTRACK	www.securitytracker.com
Microsoft Security Bulletin MS15-104 - Important Microsoft Docs	MS	docs.microsoft.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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](#)