



CVE-2015-6061

Published on: 11/11/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:16 PM UTC

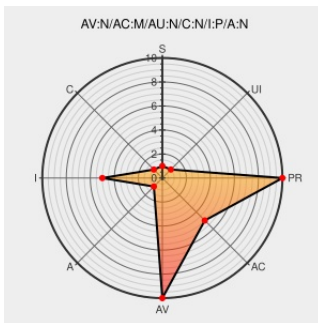
CVE-2015-6061

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

Cross-site scripting (XSS) vulnerability in Microsoft Skype for Business 2016, Lync 2010 and 2013 SP1, Lync 2010 Attendee, and Lync Room System allows remote attackers to inject arbitrary web script or HTML via an instant-message session, aka "Server Input Validation Information Disclosure Vulnerability."

CVE-2015-6061 has been assigned by secure@microsoft.com to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Microsoft Security Bulletin MS15-123 - Important Microsoft Docs	docs.microsoft.com text/html	MS MS15-123
Microsoft Lync Input Validation Flaw Lets Remote Users Obtain Potentially Sensitive Information on the Target System - SecurityTracker	www.securitytracker.com text/html	SECTRAK 1034127
Microsoft Skype for Business Input Validation Flaw Lets Remote Users Obtain Potentially Sensitive Information on the Target System - SecurityTracker	www.securitytracker.com text/html	SECTRAK 1034126

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

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	Lync Room System	-	All	All	All
Application	Microsoft	Lync Room System	-	All	All	All
Application	Microsoft	Skype For Business	2016	All	All	All
Application	Microsoft	Skype For Business	2016	All	All	All

cpe:2.3:a:microsoft:lync:2010:*:*:*:*:x64.*:

```
cpe:2.3:a:microsoft:lync:2010:*:*:*:*:x86:*:
```

cpe:2.3:a:microsoft:lync:2010:*:*:*attendee:*:*:

cpe:2.3:a:microsoft:lync:2013:sp1:*:*:*:*:x64:*:

```
cpe:2.3:a:microsoft:lync:2013:sp1:*:*:*:*:x86:*:
```

```
cpe:2.3:a:microsoft:lync:2010:*:*:*:*:x64:*:
```

```
cpe:2.3:a:microsoft:lync:2010:*:*:*:*:x86:*:
```

cpe:2.3:a:microsoft:lync:2010:*:*:*:attendee:*:*:

cpe:2.3:a:microsoft:lync:2013:sp1:*:*:*:*:x64:*:

cpe:2.3:a:microsoft:lync:2013:sp1:*:*:*:*:x86:*:

```
cpe:2.3:a:microsoft:lync_room_system:-:*:*:*:*:*:
```

```
cpe:2.3:a:microsoft:lync_room_system:-:*:*:*:*:*:
```

```
cpe:2.3:a:microsoft:skype_for_business:2016:*:*:*:*:*.*
```

cpe:2.3:a:microsoft:skype_for_business:2016:*:*:*:*:*:

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](#)