

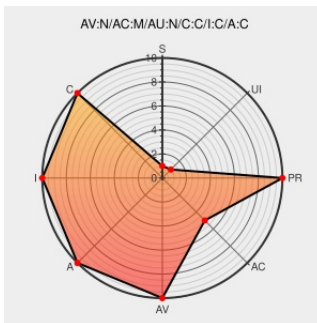


CVE-2015-6107

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

Last Modified on: 03/23/2021 11:26:17 PM UTC

CVE-2015-6107

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

The Windows font library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, Windows 10 Gold and 1511, Office 2007 SP3, Office 2010 SP2, Word Viewer, Skype for Business 2016, Lync 2010, Lync 2013 SP1, and Live

Meeting 2007 Console allows remote attackers to execute arbitrary code via a crafted embedded font, aka "Graphics Memory Corruption Vulnerability."

CVE-2015-6107 has been assigned by secure@microsoft.com to track the vulnerability

CVSS2 Score: **9.3 - HIGH**

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

CVE References

Description	Tags	Link
Microsoft Skype Font File Processing Flaw Lets Remote Users Execute Arbitrary Code - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTrack 1034332
Microsoft Lync Font File Processing Flaws Let Remote Users Execute Arbitrary Code - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTrack 1034331
Microsoft Security Bulletin MS15-128 - Critical Microsoft Docs	Patch Vendor Advisory	MS MS15-128

docs.microsoft.com
[text/html](#)

Microsoft Graphics Component Font File Processing Flaw Lets Remote Users Execute Arbitrary Code - SecurityTracker

[Third Party Advisory](#)
[VDB Entry](#)
www.securitytracker.com
[text/html](#)

 **SECTRAK**
1034336

Microsoft Office Font File Processing Flaws Let Remote Users Execute Arbitrary Code - SecurityTracker

[Third Party Advisory](#)
[VDB Entry](#)
www.securitytracker.com
[text/html](#)

 **SECTRAK**
1034333

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
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	2013	sp1	All	All
Application	Microsoft	Lync	2010	All	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	2007	sp3	All	All
Application	Microsoft	Office	2010	sp2	All	All
Application	Microsoft	Skype For Business	2016	All	All	All
Application	Microsoft	Skype For Business	2016	All	All	All
Operating System	Microsoft	Windows 10	-	All	All	All
Operating System	Microsoft	Windows 10	1511	All	All	All
Operating System	Microsoft	Windows 10	-	All	All	All
Operating System	Microsoft	Windows 10	1511	All	All	All
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 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 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
Application	Microsoft	Word Viewer	-	All	All	All
Application	Microsoft	Word Viewer	-	All	All	All
cpe:2.3:a:microsoft:live_meeting:2007:*****:						
cpe:2.3:a:microsoft:live meeting:2007:*****:						

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

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

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

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

cpe:2.3:a:microsoft:office:2007:sp3:*:*:*:*:*:

cpe:2.3:a:microsoft:office:2010:sp2:*:*:*:*:*:

cpe:2.3:a:microsoft:office:2007:sp3:*:*:*:*:*:

cpe:2.3:a:microsoft:office:2010:sp2:*:*:*:*:*:

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

```
cpe:2.3:a:microsoft:skype for business:2016:*:*:*:*:*.*
```

```
cpe:2.3:o:microsoft:windows_10:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_10:1511:*:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_10:-:*:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_10:1511:*. *. *. *. *. *. *. *
```

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

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)