



CVE-2018-8474

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

Summary

CVE	CVE-2018-8474
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-09-13 00:29:00 UTC
Updated	2019-02-28 16:28:00 UTC
Description	A security feature bypass vulnerability exists when Lync for Mac 2011 fails to properly sanitize specially crafted messages,

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Lync For Mac	2011	All	All	All
Application	Microsoft	Lync For Mac	2011	All	All	All

References

Reference	Source
Microsoft Lync for Mac 2011 - Injection Forced Browsing/Download - Windows dos Exploit	EXPLC
Microsoft Lync for Mac CVE-2018-8474 Security Bypass Vulnerability	BID
portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8474	CONF
Microsoft Lync for Mac Lets Remote Users Bypass Security Restrictions and Download Files to the Target System - SecurityTracker	SECTF
CVE Program record	CVE.C
NVD vulnerability detail	NVD

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](#).

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