



# CVE-2012-2520

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2012-2520
<b>State</b>	PUBLIC
<b>Assigner</b>	secure@microsoft.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2012-10-09 21:55:00 UTC
<b>Updated</b>	2018-10-12 22:03:00 UTC
<b>Description</b>	Cross-site scripting (XSS) vulnerability in Microsoft InfoPath 2007 SP2 and SP3 and 2010 SP1, Communicator 2007 R2, Ly

## Risk And Classification

### Problem Types: CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Groove Server	2010	sp1	All	All
Application	Microsoft	Groove Server	2010	sp1	All	All
Application	Microsoft	Infopath	2007	sp2	All	All
Application	Microsoft	Infopath	2010	sp1	All	All
Application	Microsoft	Infopath	2007	sp2	All	All
Application	Microsoft	Infopath	2010	sp1	All	All
Application	Microsoft	Lync	2010	All	All	All
Application	Microsoft	Lync	2010	All	attendee	All
Application	Microsoft	Lync	2010	All	All	All
Application	Microsoft	Lync	2010	All	attendee	All
Application	Microsoft	Office Communicator	2007	r2	All	All
Application	Microsoft	Office Communicator	2007	r2	All	All
Application	Microsoft	Office Web Apps	2010	sp1	All	All
Application	Microsoft	Office Web Apps	2010	sp1	All	All
Application	Microsoft	Sharepoint Foundation	2010	sp1	All	All
Application	Microsoft	Sharepoint Foundation	2010	sp1	All	All
Application	Microsoft	Sharepoint Server	2007	sp2	All	All

Application	Microsoft	Sharepoint Server	2007	sp3	All	All
Application	Microsoft	Sharepoint Server	2010	sp1	All	All
Application	Microsoft	Sharepoint Server	2007	sp2	All	All
Application	Microsoft	Sharepoint Server	2007	sp3	All	All
Application	Microsoft	Sharepoint Server	2010	sp1	All	All
Application	Microsoft	Sharepoint Services	3.0	sp2	All	All
Application	Microsoft	Sharepoint Services	3.0	sp2	All	All

## References

Reference	Source	Link
Microsoft Groove Server HTML Sanitizer Flaw Permits Cross-Site Scripting Attacks - SecurityTracker	SECTRACK	<a href="http://www.securitytrac">www.securitytrac</a>
Microsoft Office Communicator HTML Sanitizer Flaw Permits Cross-Site Scripting Attacks - SecurityTracker	SECTRACK	<a href="http://www.securitytrac">www.securitytrac</a>
Microsoft SharePoint HTML Sanitizer Flaw Permits Cross-Site Scripting Attacks - SecurityTracker	SECTRACK	<a href="http://www.securitytrac">www.securitytrac</a>
Repository / Oval Repository	OVAL	<a href="http://oval.cisecurity.or">oval.cisecurity.or</a>
Microsoft Security Bulletin MS12-066 - Important   Microsoft Docs	MS	<a href="http://docs.microsoft.c">docs.microsoft.c</a>
US-CERT Alert TA12-283A - Microsoft Updates for Multiple Vulnerabilities	CERT	<a href="http://www.us-cert.gov">www.us-cert.gov</a>
Microsoft SharePoint And Microsoft Lync HTML Sanitization Cross Site Scripting Vulnerability	BID	<a href="http://www.securityfoc">www.securityfoc</a>
Microsoft Lync HTML Sanitizer Flaw Permits Cross-Site Scripting Attacks - SecurityTracker	SECTRACK	<a href="http://www.securitytrac">www.securitytrac</a>
Microsoft Office InfoPath HTML Sanitizer Flaw Permits Cross-Site Scripting Attacks - SecurityTracker	SECTRACK	<a href="http://www.securitytrac">www.securitytrac</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

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](http://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](http://www.mitre.org). This site includes MITRE data granted under the following [license](http://www.mitre.org).

**CVE.report and Source URL Uptime Status** [status.cve.report](http://status.cve.report)