



CVE-2013-7485

Published on: 01/02/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:34 PM UTC

CVE-2013-7485

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Open-xchange Appsuite](#) from [Open-xchange](#) contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in the backend in Open-Xchange (OX) AppSuite 7.2.x before 7.2.2-rev26 and 7.4.x before 7.4.0-rev16 allows remote attackers to inject arbitrary web script or HTML via the publication name, which is not properly handled in an error message. NOTE: this vulnerability was SPLIT from CVE-2013-6242 because it affects different sets of versions.

CVE-2013-7485 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

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
Security Advisory SA55837 - OX App Suite Cross-Site Scripting and Script Insertion Two Vulnerabilities -	Third Party Advisory web.archive.org	SECUNIA 55837

Secunia	text/html	
No Description Provided	Broken Link xforce.iss.net Inactive Link Not Archived	🌐 XF openexchange-appsuite-url-xss(89251)
Open-Xchange frontend6 6.22.4 / backend 7.4.0 Cross Site Scripting ≈ Packet Storm	Third Party Advisory VDB Entry packetstormsecurity.com text/html	📁 MISC packetstormsecurity.com/files/124185/Open-Xchange-frontend6-6.22.4-backend-7.4.0-Cross-Site-Scripting.html
Bugtraq: Open-Xchange Security Advisory 2013-11-25	Mailing List Third Party Advisory seclists.org text/html	📁 BUGTRAQ 20131125 Open-Xchange Security Advisory 2013-11-25
Open-Xchange releases Security Patch 2013-10-30 for v7.2.2 and v7.4.0 - Official Open-Xchange Forum	Vendor Advisory forum.open-xchange.com text/html	📁 CONFIRM forum.open-xchange.com/showthread.php?8090-Open-Xchange-releases-Security-Patch-2013-10-30-for-v7-2-2-and-v7-4-0
No Description Provided	Broken Link osvdb.org Inactive Link Not Archived	🌐 OSVDB 100385
No Description Provided	Broken Link xforce.iss.net Inactive Link Not Archived	🌐 XF openexchange-cve20136242-xss(89250)
Open-Xchange Input Validation Flaws Permit Cross-Site Scripting Attacks - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	🌐 SECTrack 1029394

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	Open-xchange	Open-xchange Appsuite	7.2.2	All	All	All
Application	Open-xchange	Open-xchange Appsuite	7.4.0	All	All	All
Application	Open-xchange	Open-xchange Appsuite	7.2.2	All	All	All
Application	Open-xchange	Open-xchange Appsuite	7.4.0	All	All	All
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.2.2:*:*:*:*:*.*						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.4.0:*:*:*:*:*.*						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.2.2:*:*:*:*:*.*						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.4.0:*:*:*:*:*.*						

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.4.0:*:*:*:*
```

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