



CVE-2016-5124

Published on: 12/15/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:10 PM UTC

CVE-2016-5124

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

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

An issue was discovered in Open-Xchange OX App Suite before 7.8.1-rev14. Adding images from external sources to HTML editors by drag&drop can potentially lead to script code execution in the context of the active user. To exploit this, a user needs to be tricked to use an image from a specially crafted website and add it to HTML editor areas

of OX App Suite, for example E-Mail Compose or OX Text. This specific attack circumvents typical XSS filters and detection mechanisms since the code is not loaded from an external service but injected locally. Malicious script code can be executed within a user's context. This can lead to session hijacking or triggering unwanted actions via the web interface (sending mail, deleting data etc.). To exploit this vulnerability, a attacker needs to convince a user to follow specific steps (social-engineering).

CVE-2016-5124 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
Open-Xchange App Suite 7.8.1 Cross Site Scripting ~ Packet Storm	Third Party Advisory VDB Entry packetstormsecurity.com text/html	 CONFIRM packetstormsecurity.com/files/137894/Open-Xchange-App-Suite-7.8.1-Cross-Site-Scripting.html
SecurityFocus	www.securityfocus.com text/html	 BUGTRAQ 20160713 Open-Xchange Security Advisory 2016-07-13
Open-Xchange App Suite Input Validation Flaws Let Remote Conduct Cross-Site Scripting Attacks - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	 SECTRAK 1036296
Open-Xchange AppSuite CVE-2016-5124 Multiple Cross Site Scripting Vulnerabilities	Third Party Advisory VDB Entry cve.report (archive) text/html	 BID 91775

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	All	rev12	All	All
cpe:2.3:a:open-xchange:open-xchange_appsuite:*:rev12:*:*:*:*:						

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](#)