



CVE-2018-5754

Published on: 06/15/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:44 PM UTC

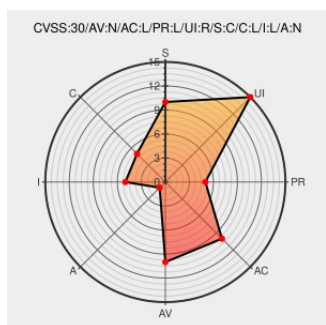
CVE-2018-5754

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 office-web component in Open-Xchange OX App Suite before 7.8.3-rev12 and 7.8.4 before 7.8.4-rev9 allows remote attackers to inject arbitrary web script or HTML via a crafted presentation file, related to copying content to the clipboard.

CVE-2018-5754 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.4 - MEDIUM**

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

CVSS2 Score: **3.5 - LOW**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Full Disclosure: Open-Xchange Security Advisory 2018-06-08	Exploit Mailing List Third Party Advisory	FULLDISC 20180608 Open-Xchange Security Advisory 2018-06-08

[seclists.org](#)
[text/html](#)

OX App Suite 7.8.4 - Multiple Vulnerabilities - XML webapps Exploit

[Exploit](#)
[Third Party Advisory](#)
[VDB Entry](#)
[www.exploit-db.com](#)
[Proof of Concept](#)
[text/html](#)

 [EXPLOIT-DB 44881](#)

OX App Suite 7.8.4 XSS / Privilege Management / SSRF / Traversal ≈ Packet Storm

[Exploit](#)
[Third Party Advisory](#)
[VDB Entry](#)
[packetstormsecurity.com](#)
[text/html](#)

 [MISC packetstormsecurity.com/files/148118/OX-App-Suite-7.8.4-XSS-Privilege-Management-SSRF-Traversal.html](#)

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	7.8.3	rev10	All	All
Application	Open-xchange	Open-xchange Appsuite	7.8.3	rev11	All	All
Application	Open-xchange	Open-xchange Appsuite	7.8.3	rev5	All	All
Application	Open-xchange	Open-xchange Appsuite	7.8.3	rev6	All	All
Application	Open-xchange	Open-xchange Appsuite	7.8.3	rev8	All	All
Application	Open-xchange	Open-xchange Appsuite	7.8.3	rev9	All	All
Application	Open-xchange	Open-xchange Appsuite	7.8.4	All	All	All
Application	Open-xchange	Open-xchange Appsuite	7.8.4	rev3	All	All
Application	Open-xchange	Open-xchange Appsuite	7.8.4	rev4	All	All
Application	Open-xchange	Open-xchange Appsuite	7.8.4	rev5	All	All
Application	Open-xchange	Open-xchange Appsuite	7.8.4	rev6	All	All
Application	Open-xchange	Open-xchange Appsuite	7.8.4	rev7	All	All
Application	Open-xchange	Open-xchange Appsuite	7.8.4	rev8	All	All
Application	Open-xchange	Open-xchange Appsuite	7.8.3	rev10	All	All
Application	Open-xchange	Open-xchange Appsuite	7.8.3	rev11	All	All
Application	Open-xchange	Open-xchange Appsuite	7.8.3	rev5	All	All
Application	Open-xchange	Open-xchange Appsuite	7.8.3	rev6	All	All
Application	Open-xchange	Open-xchange Appsuite	7.8.3	rev8	All	All
Application	Open-xchange	Open-xchange Appsuite	7.8.3	rev9	All	All
Application	Open-xchange	Open-xchange Appsuite	7.8.4	All	All	All

Application	Open-xchange	Open-xchange Appsuite	7.8.4	rev3	All	All
Application	Open-xchange	Open-xchange Appsuite	7.8.4	rev4	All	All
Application	Open-xchange	Open-xchange Appsuite	7.8.4	rev5	All	All
Application	Open-xchange	Open-xchange Appsuite	7.8.4	rev6	All	All
Application	Open-xchange	Open-xchange Appsuite	7.8.4	rev7	All	All
Application	Open-xchange	Open-xchange Appsuite	7.8.4	rev8	All	All
Application	Open-xchange	Open-xchange Appsuite	All	All	All	All
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.8.3:rev10:*****:						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.8.3:rev11:*****:						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.8.3:rev5:*****:						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.8.3:rev6:*****:						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.8.3:rev8:*****:						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.8.3:rev9:*****:						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.8.4:*****:						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.8.4:rev3:*****:						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.8.4:rev4:*****:						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.8.4:rev5:*****:						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.8.4:rev6:*****:						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.8.4:rev7:*****:						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.8.4:rev8:*****:						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.8.3:rev10:*****:						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.8.3:rev11:*****:						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.8.3:rev5:*****:						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.8.3:rev6:*****:						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.8.3:rev8:*****:						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.8.3:rev9:*****:						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.8.4:*****:						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.8.4:rev3:*****:						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.8.4:rev4:*****:						

