

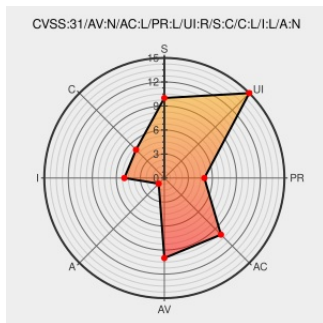


CVE-2020-8542

Published on: 06/16/2020 12:00:00 AM UTC

Last Modified on: 04/08/2022 10:37:00 AM UTC

CVE-2020-8542

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

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

OX App Suite through 7.10.3 allows XSS.

CVE-2020-8542 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
OPEN-XCHANGETM : The Collaboration and Integration Server Environment	Product www.open-xchange.com text/html	OX MISC www.open-xchange.com/
Full Disclosure: Open-Xchange Security Advisory	seclists.org	FULLDISC 20200821 Open-Xchange Security Advisory

2020-08-20

text/html

Third Party Advisory

VDB Entry

packetstormsecurity.com

text/html

2020-08-20

OX App Suite / OX Documents 7.10.3 XSS / SSRF / Improper Validation ≈ Packet Storm

MISC packetstormsecurity.com/files/158070/OX-App-Suite-OX-Documents-7.10.3-XSS-SSRF-Improper-Validation.html

OX App Suite / OX Documents XSS / SSRF / Bypass ≈ Packet Storm

packetstormsecurity.com

text/html

MISC packetstormsecurity.com/files/158932/OX-App-Suite-OX-Documents-XSS-SSRF-Bypass.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	7.10.1	-	All	All
Application	Open-xchange	Open-xchange Appsuite	7.10.1	rev1	All	All
Application	Open-xchange	Open-xchange Appsuite	7.10.1	rev10	All	All
Application	Open-xchange	Open-xchange Appsuite	7.10.1	rev11	All	All
Application	Open-xchange	Open-xchange Appsuite	7.10.1	rev12	All	All
Application	Open-xchange	Open-xchange Appsuite	7.10.1	rev13	All	All
Application	Open-xchange	Open-xchange Appsuite	7.10.1	rev14	All	All
Application	Open-xchange	Open-xchange Appsuite	7.10.1	rev15	All	All
Application	Open-xchange	Open-xchange Appsuite	7.10.1	rev16	All	All
Application	Open-xchange	Open-xchange Appsuite	7.10.1	rev17	All	All
Application	Open-xchange	Open-xchange Appsuite	7.10.1	rev18	All	All
Application	Open-xchange	Open-xchange Appsuite	7.10.1	rev19	All	All
Application	Open-xchange	Open-xchange Appsuite	7.10.1	rev2	All	All
Application	Open-xchange	Open-xchange Appsuite	7.10.1	rev20	All	All
Application	Open-xchange	Open-xchange Appsuite	7.10.1	rev21	All	All
Application	Open-xchange	Open-xchange Appsuite	7.10.1	rev22	All	All
Application	Open-xchange	Open-xchange Appsuite	7.10.1	rev23	All	All
Application	Open-xchange	Open-xchange Appsuite	7.10.1	rev24	All	All
Application	Open-xchange	Open-xchange Appsuite	7.10.1	rev25	All	All
Application	Open-xchange	Open-xchange Appsuite	7.10.1	rev26	All	All
Application	Open-xchange	Open-xchange Appsuite	7.10.1	rev27	All	All
Application	Open-xchange	Open-xchange Appsuite	7.10.1	rev3	All	All
Application	Open-xchange	Open-xchange Appsuite	7.10.1	rev4	All	All

[illegible]

cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev24:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev25:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev26:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev27:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev3:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev4:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev5:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev6:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev7:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev8:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev9:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev1:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev10:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev11:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev12:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev13:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev14:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev15:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev16:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev17:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev18:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev19:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev2:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev3:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev4:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev5:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev6:*****:

cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev7:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev8:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev9:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.3:-:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.3:rev1:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.3:rev2:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.3:rev3:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.3:rev4:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.3:rev5:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:-:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev1:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev10:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev11:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev12:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev13:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev14:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev15:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev16:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev17:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev18:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev19:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev2:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev20:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev21:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev22:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev23:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev24:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev25:*****:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev26:*****:

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev26:: : : : : :
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev27:*:*:*:*:*:
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev3:*:*:*:*:*
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev4:*:*:*:*:
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev5:*:*:*:*:
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev6:*:*:*:*:
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev7:*:*:*:*:
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev8:*:*:*:*:
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.1:rev9:*:*:*:*:
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:-:*:*:*:*.*
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev1:::*.*.*.*
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev10:*.***.***:
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev11:*:*:*:*:
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev12:*:*:*:*:
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev13:*:*:*:*:
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev14:*:*:*:*:*:
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev15:*:*:*:*:*:
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev16:*.***.*.*.*
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev17:*.***.*.*.*
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev18:*.***.*.*.*
```

```
cpe:2.3:a:open-xchange:open-xchange appsuite:7.10.2:rev19:*:*:*:*.*
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev2:*:*:*:*:*
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev3:*:*:*:*:*
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev4:*:*:*:*.*
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev5:*:*:*:*.*
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev6:::*.*.*.*.*
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev7:::*.*.*.*.*
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev8:*:*:*:*.*
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.2:rev9:::*.*.*.*.*
```


cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.3:-:*:*:*:*:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.3:rev1:*:*:*:*:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.3:rev2:*:*:*:*:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.3:rev3:*:*:*:*:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.3:rev4:*:*:*:*:
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.10.3:rev5:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

[← Previous ID](#)

[Next ID→](#)