



CVE-2014-5236

Published on: 01/31/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:53 PM UTC

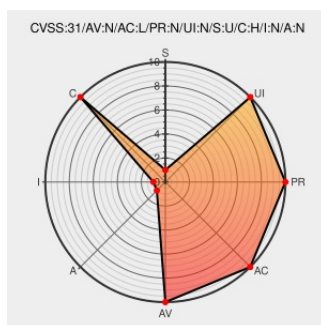
CVE-2014-5236

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

Multiple absolute path traversal vulnerabilities in documentconverter in Open-Xchange (OX) AppSuite before 7.4.2-rev10 and 7.6.x before 7.6.0-rev10 allow remote attackers to read application files via a full pathname in a crafted (1) OLE Object or (2) image in an OpenDocument text file.

CVE-2014-5236 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

Attack Vector

Attack Complexity

Privileges Required

User Interaction

NETWORK

LOW

NONE

NONE

Scope

Confidentiality Impact

Integrity Impact

Availability Impact

UNCHANGED

HIGH

NONE

NONE

CVSS2 Score: **5 - MEDIUM**

Access Vector

Access Complexity

Authentication

NETWORK

LOW

NONE

Confidentiality Impact

Integrity Impact

Availability Impact

PARTIAL

NONE

NONE

CVE References

Description

Tags

Link

[Release Notes](#)

[Vendor Advisory](#)

[software.open-xchange.com](#)

[MISC software.open-xchange.com/OX6/doc/Release_Notes_for_Patch_Release_2112_7.6.0_2014-08-25.pdf](#)

application/pdf

SecurityFocus

Third Party Advisory

 MISC www.securityfocus.com/archive/1/archive/1/533443/100/0/threaded

VDB Entry

www.securityfocus.com

text/html

Open-Xchange 7.6.0 XSS /
SSRF / Traversal ≈ Packet
Storm

Third Party Advisory

 MISC packetstormsecurity.com/files/128257/Open-Xchange-7.6.0-XSS-SSRF-Traversal.html

VDB Entry

packetstormsecurity.com

text/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	7.4.2	All	All	All
Application	Open-xchange	Open-xchange Appsuite	7.4.2	revision1	All	All
Application	Open-xchange	Open-xchange Appsuite	7.4.2	revision10	All	All
Application	Open-xchange	Open-xchange Appsuite	7.4.2	revision2	All	All
Application	Open-xchange	Open-xchange Appsuite	7.4.2	revision3	All	All
Application	Open-xchange	Open-xchange Appsuite	7.4.2	revision4	All	All
Application	Open-xchange	Open-xchange Appsuite	7.4.2	revision5	All	All
Application	Open-xchange	Open-xchange Appsuite	7.4.2	revision6	All	All
Application	Open-xchange	Open-xchange Appsuite	7.4.2	revision7	All	All
Application	Open-xchange	Open-xchange Appsuite	7.4.2	revision8	All	All
Application	Open-xchange	Open-xchange Appsuite	7.4.2	revision9	All	All
Application	Open-xchange	Open-xchange Appsuite	7.6.0	All	All	All
Application	Open-xchange	Open-xchange Appsuite	7.6.0	revision1	All	All
Application	Open-xchange	Open-xchange Appsuite	7.6.0	revision2	All	All
Application	Open-xchange	Open-xchange Appsuite	7.6.0	revision3	All	All
Application	Open-xchange	Open-xchange Appsuite	7.6.0	revision4	All	All
Application	Open-xchange	Open-xchange Appsuite	7.6.0	revision5	All	All
Application	Open-xchange	Open-xchange Appsuite	7.6.0	revision6	All	All
Application	Open-xchange	Open-xchange Appsuite	7.6.0	revision7	All	All
Application	Open-xchange	Open-xchange Appsuite	7.6.0	revision8	All	All
Application	Open-xchange	Open-xchange Appsuite	7.4.2	All	All	All
Application	Open-xchange	Open-xchange Appsuite	7.4.2	revision1	All	All

Application	Open-xchange	Open-xchange Appsuite	7.4.2	revision10	All	All
Application	Open-xchange	Open-xchange Appsuite	7.4.2	revision2	All	All
Application	Open-xchange	Open-xchange Appsuite	7.4.2	revision3	All	All
Application	Open-xchange	Open-xchange Appsuite	7.4.2	revision4	All	All
Application	Open-xchange	Open-xchange Appsuite	7.4.2	revision5	All	All
Application	Open-xchange	Open-xchange Appsuite	7.4.2	revision6	All	All
Application	Open-xchange	Open-xchange Appsuite	7.4.2	revision7	All	All
Application	Open-xchange	Open-xchange Appsuite	7.4.2	revision8	All	All
Application	Open-xchange	Open-xchange Appsuite	7.4.2	revision9	All	All
Application	Open-xchange	Open-xchange Appsuite	7.6.0	All	All	All
Application	Open-xchange	Open-xchange Appsuite	7.6.0	revision1	All	All
Application	Open-xchange	Open-xchange Appsuite	7.6.0	revision2	All	All
Application	Open-xchange	Open-xchange Appsuite	7.6.0	revision3	All	All
Application	Open-xchange	Open-xchange Appsuite	7.6.0	revision4	All	All
Application	Open-xchange	Open-xchange Appsuite	7.6.0	revision5	All	All
Application	Open-xchange	Open-xchange Appsuite	7.6.0	revision6	All	All
Application	Open-xchange	Open-xchange Appsuite	7.6.0	revision7	All	All
Application	Open-xchange	Open-xchange Appsuite	7.6.0	revision8	All	All
Application	Open-xchange	Open-xchange Appsuite	All	All	All	All
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.4.2:*****:.*:						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.4.2:revision1:*****:.*:						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.4.2:revision10:*****:.*:						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.4.2:revision2:*****:.*:						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.4.2:revision3:*****:.*:						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.4.2:revision4:*****:.*:						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.4.2:revision5:*****:.*:						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.4.2:revision6:*****:.*:						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.4.2:revision7:*****:.*:						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.4.2:revision8:*****:.*:						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.4.2:revision9:*****:.*:						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.6.0:*****:.*:						
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.6.0:revision1:*****:.*:						

```
cpe:2.3:a:open-xchange:open-xchange appsuite:7.6.0:revision2:*:*:*:*:
```

```
cpe:2.3:a:open-xchange:open-xchange appsuite:7.6.0:revision3:*.x.x.x.x:
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.6.0:revision4:*:*:*:*:
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.6.0:revision5:*:*:*:*:
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.6.0:revision6:*.***.*.*:
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.6.0:revision7:*:*:*:*:
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.6.0:revision8:*.x.x.x.x:
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.4.2:*:*:*:*:*.*
```

```
cpe:2.3:a:open-xchange:open-xchange appsuite:7.4.2:revision1:*.x.x.x.x:
```

```
cpe:2.3:a:open-xchange:open-xchange appsuite:7.4.2:revision10:*.***.***:
```

```
cpe:2.3:a:open-xchange:open-xchange appsuite:7.4.2:revision2:*.x.x.x.x:
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.4.2:revision3:*:*:*:*:
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.4.2:revision4:*:*:*:*:
```

```
cpe:2.3:a:open-xchange:open-xchange appsuite:7.4.2:revision5:*.***.***:
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.4.2:revision6:*.x.x.x.x:
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.4.2:revision7:::*.*.*.*.*
```

```
cpe:2.3:a:open-xchange:open-xchange appsuite:7.4.2:revision8:*.x.x.x.x:
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.4.2:revision9:*.***.***:
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.6.0:*:*:*:*:*:
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.6.0:revision1:*.~*~*~*~*
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.6.0:revision2:*.x.x.x.x:
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.6.0:revision3:*:*:*:*:
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.6.0:revision4:*:*:*:*:
```

```
cpe:2.3:a:open-xchange:open-xchange appsuite:7.6.0:revision5:*.***.***:
```

```
cpe:2.3:a:open-xchange:open-xchange appsuite:7.6.0:revision6::*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.6.0:revision7:*:*:*:*:
```

```
cpe:2.3:a:open-xchange:open-xchange_appsuite:7.6.0:revision8:*:*:*:*:
```

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

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](#)