Open-Xchange Security Advisory 2022-07-21

From: Martin Heiland via Fulldisclosure <fulldisclosure () seclists org>
Date: Thu, 21 Jul 2022 11:04:12 +0200 (CEST)

```
Dear subscribers,

we're sharing our latest advisory with you and like to thank everyone who contributed in
finding and solving those
vulnerabilities. Feel free to join our bug bounty programs for OX AppSuite, Dovecot and
PowerDNS at HackerOne.

Yours sincerely,
  Martin Heiland, Open-Xchange GmbH



Product: OX App Suite
Vendor: OX Software GmbH



Internal reference: DOCS-4106
Vulnerability type: OS Command Injection (CWE-78)
Vulnerable version: 7.10.6 and earlier
Vulnerable component: documentconverter
Report confidence: Confirmed
Solution status: Fixed by Vendor
Fixed version: 7.8.4-rev13, 7.10.3-rev6, 7.10.4-rev6, 7.10.5-rev5, 7.10.6-rev3
Vendor notification: 2022-01-10
Solution date: 2022-01-13
Public disclosure: 2022-07-21
CVE reference: CVE-2022-23100
CVSS: 8.2 (CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:L)

Vulnerability Details:
OX Documentconverter has a Remote Code Execution flaw that allows authenticated OX App
Suite users to run commands on
the instance which runs OX Documentconverter if they have the ability to perform document
conversions, for example of
E-Mail attachments or OX Drive content.

Risk:
Attackers can inject arbitrary operating-system level commands via OX App Suite API and/or
OX Documentconverter API.
Commands are executed on the instance running OX Documentconverter, based on "open-xchange"
```

user privileges. This can
be used to modify or exfiltrate configuration files as well as adversely affect the
instances availability by excessive
resource usage. By default the vulnerable Documentconverter API is not publicly accessible,
however this might be
worked around by abusing other weaknesses, configuration flaws or social engineering.

Steps to reproduce:
1. Create a forged Documentconverter API call that embeds escape characters and a system
command
2. Inject the malicious API call via App Suite as a proxy or other means

Solution:
We reduceed available API parameters to a limited set of enumerations, rather than
accepting API input.

Internal reference: MWB-1350
Vulnerability type: Cross-Site Scripting (CWE-80)
Vulnerable version: 7.10.6 and earlier
Vulnerable component: backend
Report confidence: Confirmed
Solution status: Fixed by Vendor
Fixed version: 7.8.4-rev78, 7.10.3-rev38, 7.10.4-rev31, 7.10.5-rev37, 7.10.6-rev9
Vendor notification: 2021-11-30
Solution date: 2022-02-15
Public disclosure: 2022-07-21
CVE reference: CVE-2022-23099
CVSS: 3.5 (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N)

Vulnerability Details:
Existing sanitization and filtering mechanisms for HTML files can be bypassed by forcing
block-wise read. Using this
technique, the recognition procedure misses to detect tags and attributes that span
multiple blocks.

Risk:
Malicious script code can be executed within a users context. This can lead to session
hijacking or triggering unwanted
actions via the web interface (e.g. redirecting to a third-party site). To exploit this an
attacker would require the
victim to follow a hyperlink.

Steps to reproduce:
1. As attacker, create a HTML malicious code-snippet which masks tags (e.g. <script>) by
block boundaries
2. Upload the code snippet to drive and create a sharing link
3. Sent that link to a victim and make it follow it

Solution:
We now check for possible HTML content through overlapping reads from data streams.

Internal reference: MWB-1366
Vulnerability type: n/a

Vulnerable version: 7.10.6 and earlier
Vulnerable component: middleware
Report confidence: Confirmed
Solution status: Fixed by Vendor
Fixed version: 7.8.4-rev78, 7.10.3-rev38, 7.10.4-rev31, 7.10.5-rev38, 7.10.6-rev9
Vendor notification: 2021-12-10
Solution date: 2022-02-15
Public disclosure: 2022-07-21
CVE reference: CVE-2021-42550
CVSS: n/a

Vulnerability Details:
In the wake of the CVE-2021-44228 (Log4Shell) issue, a similar potential vulnerability at the Logback library has been
identified (LOGBACK-1591, CVE-2021-42550). At its default configuration, OX App Suite is not susceptible to this
vulnerability and there are no scenarios that require to deploy a vulnerable configuration.

Risk:
We provide this update strictly as a precaution to mitigate the possibility of a vulnerability. Exploiting
CVE-2021-42550 at this point would require privileged access to alter system configuration.

Steps to reproduce:
1. n/a

Solution:
We provided a component update to Logback 1.2.8 and slf4j 1.7.32.

Internal reference: OXUIB-1172
Vulnerability type: Cross-Site Scripting (CWE-80)
Vulnerable version: 7.10.5 and earlier
Vulnerable component: frontend
Report confidence: Confirmed
Solution status: Fixed by Vendor
Fixed version: 7.8.4-rev69, 7.10.3-rev31, 7.10.4-rev28, 7.10.5-rev30
Vendor notification: 2021-11-30
Solution date: 2022-02-15
Public disclosure: 2022-07-21
CVE reference: CVE-2022-23101
CVSS: 4.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N)

Vulnerability Details:
Deep-links within E-Mail (e.g. links to Drive files) are not checked for malicious use of the appHandler function (see
CVE-2021-38374) and may therefore be used to inject references to malicious code.

Risk:
Malicious script code can be executed within a users context. This can lead to session hijacking or triggering unwanted
actions via the web interface (e.g. redirecting to a third-party site). To exploit this an attacker would require to
forge App Suite specific mails and force the victim to follow a hyperlink.

Steps to reproduce:
1. As an attacker, create a malicious E-Mail that uses App Suite "Deep-links" as mail header and embed a call to the
AppLoader component
2. Deliver the mail and make the victim open the link

Proof of concept:
X-Open-Xchange-Share-URL:
https://example.com/#!!&app=%2e./%2e./%2e./%2e./%2e./%2e./appsuite/drive/script.js?cut=&id=123

Solution:
We now check for a enumeration of valid applications for deep-links as well.

Internal reference: DOCS-4161
Vulnerability type: OS Command Injection (CWE-78)
Vulnerable version: 7.10.6 and earlier
Vulnerable component: documentconverter
Report confidence: Confirmed
Solution status: Fixed by Vendor
Fixed version: 7.8.4-rev14, 7.10.3-rev7, 7.10.4-rev7, 7.10.5-rev6, 7.10.6-rev3
Vendor notification: 2022-01-24
Solution date: 2022-02-15
Public disclosure: 2022-07-21
CVE reference: CVE-2022-24405
CVSS: 7.3 (CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N)

Vulnerability Details:
The compatibility layer of documentconverter API processes serialized Java classes when using remote cache calls. This
can be exploited to inject malicious code that is being executed in the context of the documentconverter component.

Risk:
Attackers can inject arbitrary operating-system level commands via the OX Documentconverter API. Commands are executed
on the instance running OX Documentconverter, based on "open-xchange" user privileges. This can be used to modify or
exfiltrate configuration files as well as adversely affect the instances availability by excessive resource usage. By
default the vulnerable OX Documentconverter API is not publicly accessible and we are not aware that this could have
been exploited without privileged network or system access.

Steps to reproduce:
1. Create a malicious Java class and serialize it
2. Use the OX Documentconverter API to inject this class as a reference/hash to remote caches

Solution:
We now apply input sanitization to this API call and retrict it to strings. We also implemented a set of additional
hardening procedures for other API calls which work in a similar way.

Internal reference: DOCS-4120
Vulnerability type: Server-Side Request Forgery (CWE-918)
Vulnerable version: 7.10.6 and earlier
Vulnerable component: documentconverter-api

```
Report confidence: Confirmed
Solution status: Fixed by Vendor
Fixed version: 7.8.4-rev10, 7.10.3-rev5, 7.10.4-rev6, 7.10.5-rev6, 7.10.6-rev3
Vendor notification: 2022-01-10
Solution date: 2022-02-15
Public disclosure: 2022-07-21
CVE reference: CVE-2022-24406
CVSS: 6.4 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N)

Vulnerability Details:
By creating colissions of HTTP multipart-formdata boundaries it is possible to alter the
API request parameters between
OX App Suite and OX Documentconverter. Legitimate multipart-formdata boundaries are created
based on a timestamp with
millisecond resolution. This allows attackers to predict the next boundary and attempt to
overwrite its content. The
most practical way to exploit this is sending a large number of formdata parts, each with a
unique boundary based on a
future point in time.

Risk:
Attackers can modify parameters of internal API calls to OX Documentconverter and by that
circumvent network trust
boundaries. In effect, a server-side request forgery attack is possible, for example to
exploit DOCS-4106
(CVE-2022-23100) with limited privileges using OX App Suite API as a "proxy".

Steps to reproduce:
1. Create a HTTP request with multipart-formdata boundaries representing timestamps in the
near future
2. Add internal API parameters to those multipart-formdata sections and use them as
requests to OX App Suite API

Solution:
We modified the algorithm to create multipart-formdata boundaries in a way that they are no
longer predictable. We also
restricted the number of multipart-formdata parts to a sensible amount and issue an
Exception if a client exceeds it.
```

Attachment: **signature.asc**
Description: