

Internal reference: DOCS-3309
Vulnerability type: Relative Path Traversal (CWE-23)
Vulnerable version: 7.10.5 and earlier
Vulnerable component: office
Report confidence: Confirmed
Solution status: Fixed by Vendor
Fixed version: 7.10.3-rev15, 7.10.4-rev9, 7.10.5-rev6
Vendor notification: 2021-03-23
Solution date: 2021-06-01
Public disclosure: 2021-11-18
CVE reference: CVE-2021-33491
CVSS: 6.4 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:L/A:L)

Vulnerability Details:
External mail account discovery allows malicious users to append arbitrary URL paths to mail addresses. In combination with malicious auto-configuration DNS records, this can be abused to access web services outside of the expected trust boundary, regardless of existing blocklists.

Risk:
Zip archives (like OOXML and ODF documents) might contain entries with relative paths, pointing outside of archive root. The extraction process uses the assigned paths and make it is possible to override OX service user writable files (e.g. log files)

Steps to reproduce:
1. Create a OOXML or ODF file, modify the ZIP archive content table
2. Use a relative path that would overwrite or add files to unexpected locations
3. Use OX Documents to open such files

Proof of concept:
../tmp/foobar

Solution:
We now prevent the extraction of files with relative paths outside of the expected working directories. A WARN message has been added to the log file whenever this happens.

Internal reference: OXUIB-770
Vulnerability type: Improper Input Validation (CWE-20)
Vulnerable version: 7.10.5
Vulnerable component: frontend
Report confidence: Confirmed
Solution status: Fixed by Vendor
Fixed version: 7.10.5-rev12
Vendor notification: 2021-03-17
Solution date: 2021-06-01
Public disclosure: 2021-11-18
CVE reference: CVE-2021-33488
CVSS: 5.4 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)

Vulnerability Details:
The "chat" component contains development related hooks to provide the URL of the chat backend service. This can be used to redirect users to rogue OX Chat servers.

Risk:
User may disclose sensitive information at a non-trusted system or get harassed with unsolicited content. To exploit this an attacker would require the victim to follow a hyperlink.

Steps to reproduce:
1. Setup a rogue OX Chat backend or mock service
2. Create a hyperlink pointing to that service
3. Make users click that link

Proof of concept:
https://example.com/appsuite/#!/\$app=io.ox/chat&chatHost=https://127.0.0.1:8000

Solution:
We no longer accept user provided input as configuration for client components.

Internal reference: OXUIB-771
Vulnerability type: Cross-Site Scripting (CWE-80)
Vulnerable version: 7.10.5
Vulnerable component: backend
Report confidence: Confirmed
Solution status: Fixed by Vendor
Fixed version: 7.10.5-rev12
Vendor notification: 2021-03-17
Solution date: 2021-06-01
Public disclosure: 2021-11-18
CVE reference: CVE-2021-33492
CVSS: 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

Vulnerability Details:
Room names in OX Chat can be set to JS code fragments, those are not sufficiently sanitized before adding them to other room participants DOM.

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 need to be part of the OX context as the victim.

Steps to reproduce:
1. Create a chat room with JS code as title
2. Invite other users

Solution:
We improved sanitization of room titles since they are user-provided information.

Internal reference: OXUIB-809
Vulnerability type: Cross-Site Scripting (CWE-80)
Vulnerable version: 7.10.4 and earlier
Vulnerable component: frontend
Report confidence: Confirmed
Solution status: Fixed by Vendor
Fixed version: 7.10.3-rev30, 7.10.4-rev26
Vendor notification: 2021-04-16
Solution date: 2021-06-01
Public disclosure: 2021-11-18
CVE reference: To be assigned by the vulnerable component
CVSS: 5.3 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)

Vulnerability Details:
OX App Suite uses the "blanksheild" component to protect older browsers against "tabnabbing" attacks. A vulnerability was detected at this component, which could be used to run cross-site scripting attacks by injecting malicious hyperlinks to E-Mail and other content.

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. The issue is related to browsers which are no longer supported by OX App Suite 7.10.5 or newer.

Steps to reproduce:
1. Create a E-Mail with a hyperlink that contains malicious JS code
2. Send that E-Mail to the victim and make it follow the link

Solution:
We provided a workaround for this issue to our code and to the upstream component.

Internal reference: OXUIB-837
Vulnerability type: Cross-Site Scripting (CWE-80)
Vulnerable version: 7.10.5
Vulnerable component: frontend
Report confidence: Confirmed
Solution status: Fixed by Vendor
Fixed version: 7.10.5-rev12
Vendor notification: 2021-05-06
Solution date: 2021-06-01
Public disclosure: 2021-11-18
CVE reference: CVE-2021-33494
CVSS: 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

| | |
|------------------------|-----------------|
| Spoof (2,166) | SUSE (1,444) |
| SQL Injection (16,102) | Ubuntu (8,199) |
| TCP (2,379) | UNIX (9,159) |
| Trojan (686) | UnixWare (185) |
| UDP (676) | Windows (6,511) |
| Virus (662) | Other |
| Vulnerability (31,136) | |
| Web (9,365) | |
| Whitepaper (3,729) | |
| x86 (946) | |
| XSS (17,494) | |
| Other | |

```
Vulnerability Details:
A OX Chat method did not properly escape the room title when rendering the "typing" status and adding it to DOM.

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 need to be part of the OX context as the victim.

Steps to reproduce:
1. Create a OX Chat room with malicious code as title
2. Make users join and interact with this channel

Solution:
We now escape user input, like the room title, when injecting it to DOM.

---

Internal reference: OXUIB-838
Vulnerability type: Cross-Site Scripting (CWE-80)
Vulnerable version: 7.10.5
Vulnerable component: frontend
Report confidence: Confirmed
Solution status: Fixed by Vendor
Fixed version: 7.10.5-rev12
Vendor notification: 2021-05-06
Solution date: 2021-06-01
Public disclosure: 2021-11-18
CVE reference: CVE-2021-33495
CVSS: 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

Vulnerability Details:
A OX Chat method did not properly escape content of "system messages" when adding it to DOM.

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 need to be part of the OX context as the victim.

Steps to reproduce:
1. Create a system message in OX Chat that includes HTML/JS code
2. Make users join and interact with OX Chat

Solution:
We escape any chat messages, including system messages, when injecting it to DOM.
```

[Login](#) or [Register](#) to add favorites



© 2022 Packet Storm. All rights reserved.

Site Links


- [News by Month](#)
- [News Tags](#)
- [Files by Month](#)
- [File Tags](#)
- [File Directory](#)


About Us

- [History & Purpose](#)
- [Contact Information](#)
- [Terms of Service](#)
- [Privacy Statement](#)
- [Copyright Information](#)

Hosting By

[Rokasec](#)

 [Follow us on Twitter](#)

 [Subscribe to an RSS Feed](#)