



Site Search



[Full Disclosure](#) mailing list archives



[By Date](#) [By Thread](#)

List Archive Search



Open-Xchange Security Advisory 2021-11-19

From: Open-Xchange GmbH via Fulldisclosure <fulldisclosure () seclists.org>

Date: Fri, 19 Nov 2021 10:40:28 +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
Vendor: OX Software GmbH

Internal reference: OXUIB-872
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: 7.10.3-rev30, 7.10.4-rev27, 7.10.5-rev18
Vendor notification: 2021-06-01
Solution date: 2021-08-23
Public disclosure: 2021-11-19
CVE reference: CVE-2021-38374
CVSS: 4.3 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)

Vulnerability Details:
The "app loader" mechanism of the frontend component could be abused to load content from relative URLs, outside of the intended code loading API path. This can be used by attackers to add references to malicious content that is served by the same domain.

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, upload a code snippet to drive and create a sharing link
2. Modify the "app loader" URL and include a relative reference to the shared code snippet
3. Embed a direct reference to this snippet at a malicious website or make a user follow the reference

Solution:
We now restrict relative references to only include the intended API path.

Internal reference: MWB-1113
Vulnerability type: Cross-Site Scripting (CWE-80)
Vulnerable version: 7.10.5 and earlier
Vulnerable component: middleware
Report confidence: Confirmed
Solution status: Fixed by Vendor
Fixed version: 7.10.3-rev36, 7.10.4-rev27, 7.10.5-rev21
Vendor notification: 2021-06-02
Solution date: 2021-08-23
Public disclosure: 2021-11-19
CVE reference: CVE-2021-38375
CVSS: 4.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N)

Vulnerability Details:
HTML E-Mails with lots of content are being truncated for improved performance. Their full content is being delivered when opening the HTML part at a dedicated browser tab. The mechanism that dealt with inline images allowed to inject script code as part of a HTML img "alt" tag.

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 open the non-truncated representation of an E-Mail.

Steps to reproduce:
1. Create a artificially large HTML E-Mail with script code at an images "alt" tag.
2. Deliver the mail and make the victim display the truncated part

Proof of concept:

Solution:
We updated the detection and sanitization logic to deal with embedded script code fragments.

Internal reference: MWB-1116
Vulnerability type: Cross-Site Scripting (CWE-80)
Vulnerable version: 7.10.5 and earlier
Vulnerable component: middleware
Report confidence: Confirmed
Solution status: Fixed by Vendor
Fixed version: 7.10.3-rev36, 7.10.4-rev27, 7.10.5-rev21
Vendor notification: 2021-06-02
Solution date: 2021-08-23
Public disclosure: 2021-11-19
CVE reference: CVE-2021-38377
CVSS: 4.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N)

Vulnerability Details:
HTML E-Mails with lots of content are being truncated for improved performance. Their full content is being delivered when opening the HTML part at a dedicated browser tab. The mechanism that dealt with temporary internal transformation state allowed to inject script code by abusing a "anchor" HTML comment. The comments identifier is a predictable UUID and stores HTML transformation results, which is exempt from sanitization.

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 open the non-truncated representation of an E-Mail.

Steps to reproduce:
1. Create a artificially large HTML E-Mail with script code at an "anchor" comment
2. Deliver the mail and make the victim display the truncated part

Proof of concept:
<!--anchor-5fd15ca8-a027-4b14-93ea-35de1747419e: -->

Solution:
We now use a random value for temporary anchors to avoid exploiting this internal state.

Internal reference: MWB-1185
Vulnerability type: Information Disclosure (CWE-200)
Vulnerable version: 7.10.5 and earlier
Vulnerable component: middleware
Report confidence: Confirmed
Solution status: Fixed by Vendor
Fixed version: 7.10.3-rev36, 7.10.4-rev27, 7.10.5-rev21
Vendor notification: 2021-07-15
Solution date: 2021-08-23
Public disclosure: 2021-11-19
CVE reference: CVE-2021-38376
CVSS: 3.7 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)

Vulnerability Details:
The "rampup" API action allows to swiftly extract a predefined set of information stored with a specific user session identifier to load generic information, for example available languages and folder names. It also contains a subset of personal information like a users name and mail address. However the call is not covered by standard authentication methods, allowing to extract this information when guessing or intercepting the users session identifier.

Risk:
Unauthorized parties may get access to confidential non-public information, associated to a live user session. In order to gain access to the session identifier, an attacker requires access to infrastructure, log files or elevated privileges at either endpoints.

Steps to reproduce:
1. Find out a users session identifier
2. Use the "rampup" action of the login API call to request session information

Proof of concept:
<https://example.com/appsuite/api/login?action=rampup&rampup=true&rampUpFor=open-xchange-appsuite&sessionvb5b1ae9352b9a0b6d483b6f2f78c70>

Solution:
We applied standard authentication requirements for this API action.

Internal reference: MWB-1208
Vulnerability type: Information Disclosure (CWE-200)
Vulnerable version: 7.10.5
Vulnerable component: middleware
Report confidence: Confirmed
Solution status: Fixed by Vendor
Fixed version: 7.10.3-rev36, 7.10.4-rev27, 7.10.5-rev21
Vendor notification: 2021-08-09
Solution date: 2021-08-23
Public disclosure: 2021-11-19
CVE reference: CVE-2021-38378
CVSS: 4.3 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)

Vulnerability Details:
A caching mechanisms for files in OX Drive did not consider the context identifier of a specific object.

Risk:
Unauthorized users may get access to confidential information, like other users names, by observing the "modified by" response of the API for files that would collide with other users files that bear the same identifier. This weakness depends on chance and is limited to the names of users, there is no evidence that actual file content could have been exposed.

Steps to reproduce:
1. Create multiple files in OX Drive on a environment with many contexts
2. Observe the "modified by" information which indicates who last changed the file
3. In rare cases where identifiers collided, other users surname and givenname were shown

Solution:
We made the affected cache context-ware to avoid exposing this sort of information to unauthorized users.

Attachment: [signature.asc](#)
Description: Message signed with OpenPGP

Sent through the Full Disclosure mailing list
<https://nmap.org/mailman/listinfo/fulldisclosure>
Web Archives & RSS: <http://seclists.org/fulldisclosure/>

◀ By Date ▶ ▶ By Thread ▶

Current thread:

Open-Xchange Security Advisory 2021-11-19 *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

