OX App Suite 7.10.5 Cross Site Scripting / Information Disclosure

Authored by Martin Heiland | Posted Nov 22, 2021

OX App Suite versions 7.10.5 and below suffer from cross site scripting and information disclosure vulnerabilities.

tags | exploit, vulnerability, xss, info disclosure
advisories | CVE-2021-38374, CVE-2021-38375, CVE-2021-38376, CVE-2021-38377, CVE-2021-38378
SHA-256 | c99f2e36cd127fb981a5512d68d67833a23fbcadee9ad6f6f9c134c3632fb7ef Download | Favorite | View

Related Files

Change Mirror Download

```
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 artifically 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:
<img alt="src=foo.bar/onerror=alert('XSS')//" src="">

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 artifically 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: <img src="" onerror="alert('XSS');">-->

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
```


File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

- Red Hat 157 files
- Ubuntu 76 files
- LiquidWorm 23 files
- Debian 21 files
- nu11secur1ty 11 files
- malvuln 11 files
- Gentoo 9 files
- Google Security Research 8 files
- Julien Ahrens 4 files
- T. Weber 4 files

File Tags

- ActiveX (932)
- Advisory (79,754)
- Arbitrary (15,694)
- BBS (2,859)
- Bypass (1,619)
- CGI (1,018)
- Code Execution (6,926)
- Conference (673)
- Cracker (840)
- CSRF (3,290)
- DoS (22,602)
- Encryption (2,349)
- Exploit (50,359)
- File Inclusion (4,165)
- File Upload (946)
- Firewall (821)
- Info Disclosure (2,660)
- Intrusion Detection (867)
- Java (2,899)
- JavaScript (821)
- Kernel (6,291)
- Local (14,201)
- Magazine (586)
- Overflow (12,419)
- Perl (1,418)
- PHP (5,093)
- Proof of Concept (2,291)
- Protocol (3,435)
- Python (1,467)
- Remote (30,044)
- Root (3,504)
- Ruby (594)
- Scanner (1,631)
- Security Tool (7,777)
- Shell (3,103)
- Shellcode (1,204)
- Sniffer (886)

File Archives

- December 2022
- November 2022
- October 2022
- September 2022
- August 2022
- July 2022
- June 2022
- May 2022
- April 2022
- March 2022
- February 2022
- January 2022
- Older

Systems

- AIX (426)
- Apple (1,926)
- BSD (370)
- CentOS (55)
- Cisco (1,917)
- Debian (6,634)
- Fedora (1,690)
- FreeBSD (1,242)
- Gentoo (4,272)
- HPUX (878)
- iOS (330)
- iPhone (108)
- IRIX (220)
- Juniper (67)
- Linux (44,315)
- Mac OS X (684)
- Mandriva (3,105)
- NetBSD (255)
- OpenBSD (479)
- RedHat (12,469)
- Slackware (941)
- Solaris (1,607)

```
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 identifer, 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&session=76b5b1ae9352b9a0b6d483b6f2f78c70

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 mechanims 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.
```


Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

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