

OX App Suite / OX Guard / OX Documents SSRF / Cross Site Scripting

Authored by Martin Helland

Posted Jul 16, 2021

Open-Xchange OX App Suite, OX Guard, and OX Documents suffer from server-side request forgery and cross site scripting vulnerabilities. Some of these issues only affect version 7.10.3 while some affect 7.10.4 and earlier.

tags | exploit, vulnerability, xss

advisories | CVE-2020-24700, CVE-2020-24701, CVE-2021-26698, CVE-2021-26699

SHA-256 | 264f5c37a41ec6bca16aeacc29650f3f157abec2e181ef828458e50fe0bc2740 Download | Favorite | View

Related Files

Share This

Like

Twitter

LinkedIn

Reddit

Digg

StumbleUpon

Change Mirror

Download

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.

Note that some bugfixes (MWB-423, MWB-460, MWB-492, MWB-493 and MWB-494) have been fixed with 7.10.4 and later already. We recently provided backports to 7.10.3, thus updating the information on those vulnerabilities.

Yours sincerely,

Martin Helland, Open-Xchange GmbH

Product: OX App Suite, OX Guard, OX Documents
Vendor: OX Software GmbH

Internal reference: MWB-423
Vulnerability type: Server-Side Request Forgery (CWE-918)
Vulnerable version: 7.10.3
Vulnerable component: backend
Report confidence: Confirmed
Solution status: Fixed by Vendor
Fixed version: 7.10.3-rev32
Vendor notification: 2020-06-26
Solution date: 2021-02-10
Public disclosure: 2021-07-15
Researcher Credits: Stuart Redman
CVE reference: CVE-2020-24700
CVSS: 6.4 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N)

Vulnerability Details:

The oauth Proxy capability, used to exchange data with third-party services such as Twitter, can be abused to craft requests to services which are prohibited. These services may reside within a protected network and could be exposed using this technique. The code to check for allowed domains did not account for certain URL constructs.

Risk:

Malicious users can trigger network requests to web services outside of the expected trust boundary, for example services within a restricted network to which the OX App Suite middleware node has access. In case such services do not have further access control, a malicious user could retrieve web service content from them. The vulnerability allows to control request type and headers sent to those services.

Steps to reproduce:

1. Connect your OX App Suite account to an oauth-enabled service like Twitter
2. Forge API requests via /api/oauth/proxy containing payload related to internal services
3. API response will contain an error but also the retrieved content for the internal service

Proof of concept:

FUT https://example.com/appsuite/api/oauth/proxy?api=com.openexchange.oauth.twitter&session=XYZ
["url":"https://twitter.com@example.com","params":{"count":10,"include_entities":true}]

Solution:

We improved detection of user-provided payload when checking against access lists. Regardless of this fix we suggest tight network segmentation, egress traffic filtering and access controls for any kind of service.

Internal reference: MWB-460
Vulnerability type: Server-Side Request Forgery (CWE-918)
Vulnerable version: 7.10.3
Vulnerable component: backend
Report confidence: Confirmed
Solution status: Fixed by Vendor
Fixed version: 7.10.3-rev32
Vendor notification: 2020-07-07
Solution date: 2021-02-10
Public disclosure: 2021-07-15
CVE reference: CVE-2020-24700
CVSS: 4.3 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)

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:

Malicious users can trigger network requests to web services outside of the expected trust boundary, regardless of existing blocklists. This may be used to probe for services and paths within a restricted network to which the OX App Suite middleware node has access and potentially ease further attacks.

Steps to reproduce:

1. Setup a DNS A record for autoconfig.example.com, pointing to a local addresses like 127.0.0.1
2. Use the "external mail account" feature to setup a mail account for this domain
3. Append URL paths to the mail address, e.g. foo@example.com/ssrf/ping

Proof of concept:

DNS lookup will return "127.0.0.1" and OX App Suite will append the URL fragment of the mail address, resulting in a GET request to http://127.0.0.1/ssrf/ping?emailaddress=foo@example.com.

Solution:

We restricted the ability to access blocked networks when performing autoconfig lookups.

Internal reference: MWB-492
Vulnerability type: Cross-Site Scripting (CWE-80)
Vulnerable version: 7.10.3
Vulnerable component: backend
Report confidence: Confirmed
Solution status: Fixed by Vendor
Fixed version: 7.10.3-rev32
Vendor notification: 2020-07-20
Solution date: 2021-02-10
Public disclosure: 2021-07-15
CVE reference: CVE-2020-24701
CVSS: 4.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N)

Vulnerability Details:

The "debug" option for the /apps/manifests endpoint included request parameters in its response, without using HTML escaping.

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 150 files
Ubuntu 68 files
LiquidWorm 23 files
Debian 16 files
malvuln 11 files
nu11security 11 files
Gentoo 9 files
Google Security Research 6 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags

ActiveX (932)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (8,926)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,602)	February 2022
Encryption (2,349)	January 2022
Exploit (50,359)	Older

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 (1,600)
FreeBSD (1,242)
Genoo (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)

<p>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.</p> <p>Steps to reproduce: 1. Create a link to the /apps/manifest endpoint using the debug option and append malicious script code 2. Make a user open this link, for example through social engineering</p> <p>Proof of concept: https://example.com/ajax/apps/manifests?action=all&format-debug&xss=%3Cscript%3Ealert(%22XSS%22);%3C/script%3E</p> <p>Solution: We now escape any user-provided content when creating the debug response.</p> <p>---</p> <p>Internal reference: MWB-493 Vulnerability type: Cross-Site Scripting (CWE-80) Vulnerable version: 7.10.4 and earlier Vulnerable component: backend Report confidence: Confirmed Solution status: Fixed by Vendor Fixed version: 7.10.3-rev32 Vendor notification: 2020-07-20 Solution date: 2021-02-10 Public disclosure: 2021-07-15 CVE reference: CVE-2020-24701 CVSS: 4.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N)</p> <p>Vulnerability Details: The logic for determining safe content could be bypassed by providing unknown values for content-disposition while requesting a shared file. In case the file contained malicious script code, this would be executed.</p> <p>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.</p> <p>Steps to reproduce: 1. Create a HTML file with malicious JS code and upload it to Drive 2. Create a public sharing link 3. Modify this link to contain a unexpected content_disposition parameter value 4. Make the victim follow this link</p> <p>Proof of concept: https://example.com/ajax/share/cshare-token?delivery=viewscontent_disposition=foo</p> <p>Solution: We improved the detection mechanism to neglect user-specified parameter values.</p> <p>---</p> <p>Internal reference: MWB-494 Vulnerability type: Cross-Site Scripting (CWE-80) Vulnerable version: 7.10.3 Vulnerable component: backend Report confidence: Confirmed Solution status: Fixed by Vendor Fixed version: 7.10.3-rev32 Vendor notification: 2020-07-21 Solution date: 2021-02-10 Public disclosure: 2021-07-15 CVE reference: CVE-2020-24701 CVSS: 4.3 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)</p> <p>Vulnerability Details: Access to a cache for internal file handling (e.g. importing vcards from an E-Mail to the address book) was not restricted to specific users. While the chance of unauthorized access is very low, the attacker would have required to correctly guess a 128b UUID before the cache expires, this could be used to hide and deliver malicious script code. Content at this cache was not sanitized or filtered and direct references could be used in phishing attacks.</p> <p>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.</p> <p>Steps to reproduce: 1. Include malicious script code within external content like a vcard file 2. Attach this file to a mail and use the conversation API to create a managed distributed file 3. Find out the UUID reference to this managed "distributedFile" 4. Make the victim open this direct reference as hyperlink</p> <p>Solution: We now require user-specific authentication to access the API endpoint for managed distributed files.</p> <p>---</p> <p>Internal reference: MWB-838 Vulnerability type: Cross-Site Scripting (CWE-80) Vulnerable version: 7.10.4 and earlier Vulnerable component: backend Report confidence: Confirmed Solution status: Fixed by Vendor Fixed version: 7.10.3-rev32, 7.10.4-rev18 Vendor notification: 2021-01-04 Solution date: 2021-01-11 Public disclosure: 2021-07-15 CVE reference: CVE-2021-26698 CVSS: 3.5 (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N)</p> <p>Vulnerability Details: In case a legacy component ("dataretrieval", disabled by default) is installed and enabled, it can be exploited to serve script code that can be called by a direct reference. The component did lack proper sanitization and output filtering.</p> <p>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.</p> <p>Steps to reproduce: 1. As Operator, enable the "dataretrieval" component 2. As attacker, upload script-code as binary data 3. Distribute a direct reference to the dataretrieval endpoint to the victim 4. Make the victim open this direct reference as hyperlink</p> <p>Solution: We removed the legacy feature to avoid unintended usage. Note that this does NOT affect any GDPR related data export functionality.</p> <p>---</p> <p>Internal reference: MWB-839 Vulnerability type: Cross-Site Scripting (CWE-80) Vulnerable version: 7.10.4 and earlier Vulnerable component: backend Report confidence: Confirmed Solution status: Fixed by Vendor Fixed version: 7.10.3-rev32, 7.10.4-rev18 Vendor notification: 2021-01-04 Solution date: 2021-02-10 Public disclosure: 2021-07-15 CVE reference: CVE-2021-26698 CVSS: 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)</p> <p>Vulnerability Details: A URL parameter could be used to modify the result of existing sanitization and output handling, when downloading user-generated content.</p> <p>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.</p>	<p>Spoof (2,166)</p> <p>SQL Injection (16,102)</p> <p>TCP (2,379)</p> <p>Trojan (686)</p> <p>UDP (676)</p> <p>Virus (662)</p> <p>Vulnerability (31,136)</p> <p>Web (9,365)</p> <p>Whitepaper (3,729)</p> <p>x86 (946)</p> <p>XSS (17,494)</p> <p>Other</p>
	<p>SUSE (1,444)</p> <p>Ubuntu (8,199)</p> <p>UNIX (9,159)</p> <p>UnixWare (185)</p> <p>Windows (6,511)</p> <p>Other</p>

```
Steps to reproduce:
1. As attacker, upload a code snippet to drive and create a sharing link
2. Modify the URL parameters to include the "dl" parameter
3. Embed a direct reference to this snippet at a malicious website or make a user follow the reference

Solution:
We now ignore user-provided URL parameters when deciding how to handle output. References to shared files will
always trigger downloads.

---

Internal reference: OXUIB-645
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-rev27, 7.10.4-rev19
Vendor notification: 2021-01-04
Solution date: 2021-02-10
Public disclosure: 2021-07-15
CVE reference: CVE-2021-26698
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: DOCS-3139
Vulnerability type: Server-Side Request Forgery (CWE-918)
Vulnerable version: 7.10.4 and earlier
Vulnerable component: imageconverter
Report confidence: Confirmed
Solution status: Fixed by Vendor
Fixed version: 7.10.3-rev4, 7.10.4-rev4
Vendor notification: 2020-12-18
Solution date: 2021-02-10
Public disclosure: 2021-07-15
CVE reference: CVE-2021-26699
CVSS: 5.4 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:L)

Vulnerability Details:
SVG files are processed by the imageconverter component. In case they include references to external entities,
imageconverter would attempt to process them.

Risk:
This technique can be used to reduce availability of the environment by referencing excessive amounts of data.
It may also be used to track individual users and monitor what files they are opening using App Suite. This
would require the attacker to inject compromised images to the users workflow.

Steps to reproduce:
1. Generate a SVG file with external references, e.g. API endpoints
2. Rename the file to add a .png extension and share it on OX Drive or send by mail
3. Make the victim use the image viewer to open the file

Solution:
We now restrict relative references and block potentially harmful files from being processed as images.
```

[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