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

Authored by Martin Heiland

Posted Apr 30, 2021

OX App Suite versions 7.10.4 and below suffer from cross site scripting and server-side request forgery vulnerabilities. OX Guard versions 2.10.4 and below suffer from a denial of service vulnerability.

tags | exploit, denial of service, vulnerability, xss
advisories | CVE-2020-28943, CVE-2020-28944, CVE-2020-28945
SHA-256 | f79fdb3de2e0adf5d96f8bd0f53e9ea78572bc1ad06052cccf66726ab09192b0

Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
Product: OX App Suite / OX Guard
Vendor: OX Software GmbH



Affected product: OX App Suite
Internal reference: OXUIB-481
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-rev23, 7.10.4-rev14
Vendor notification: 2020-09-28
Solution date: 2020-11-23
Public disclosure: 2021-04-30
CVE reference: CVE-2020-28945
CVSS: 4.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N)

Vulnerability Details:
When searching for contacts in mobile mode (App Suite UI on a smartphone), specific fields of a contact object
were not properly handled. This could lead to script execution in case the users search would yield contacts
with malicious data.

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 execute a specific action.

Steps to reproduce:
1. Create a malicious contact which contains script-code as "position" or "company" value
2. Share the contact with the victim, for example within the same context or as vcard file
3. Make the victim search for this contact in mobile mode

Solution:
We improved how search results in mobile mode are being constructed and delivered, considering user-provided
information as potentially malicious.



---



Affected product: OX App Suite
Internal reference: OXUIB-491
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-rev23, 7.10.4-rev14
Vendor notification: 2020-10-01
Solution date: 2020-11-23
Public disclosure: 2021-04-30
CVE reference: CVE-2020-28945
CVSS: 4.3 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)

Vulnerability Details:
An undocumented component did not correctly handle user-generated content when displaying the information to a
user.

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 link provided by the attacker.

Steps to reproduce:
1. Create or upload a malicious "Notes" item
2. Share that item with a user within the same context and make them open it

Proof of concept:
xx ![](http://onerror=Function.constructor`\x61\x6c\x65\x72\x74\x28\x22\x58\x53\x53\x22\x29\x3b`.call``;// ) yy

Solution:
We disabled the ability to launch the undocumented component for the time being and therefore the risk of
executing malicious content as code.



---



Affected product: OX App Suite
Internal reference: OXUIB-509
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-rev23, 7.10.4-rev14
Vendor notification: 2020-10-12
Solution date: 2020-11-23
Public disclosure: 2021-04-30
CVE reference: CVE-2020-28945
CVSS: 4.3 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)

Vulnerability Details:
Contact "distribution lists" can be created in a way that they contain script code which is being executed in
"scheduling" view.

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 import data and/or execute a specific action.

Steps to reproduce:
1. Create a malicious distribution list where a member contains malicious script code as "common name"
2. Share the distribution list with the victim, for example within the same context or as vcard file
3. Make the victim add this distribution list to "scheduling" view in calendar

Proof of concept:
" " <img/src='x'/onerror='alert("XSS")'/cut=@example.com>

Solution:
We improved how the "scheduling" overview is being constructed and delivered, considering user-provided
information as potentially malicious.



---
```

Follow us on Twitter

Subscribe to an RSS Feed

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
nu11secur1ty 11 files
Gentoo 9 files
Google Security Research 6 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)

```
Affected product: OX App Suite
Internal reference: MWB-646
Vulnerability type: Server-Side Request Forgery (CWE-918)
Vulnerable version: 7.10.4 and earlier
Vulnerable component: backend
Report confidence: Confirmed
Solution status: Fixed by Vendor
Fixed version: 7.10.3-rev28, 7.10.4-rev14
Vendor notification: 2020-10-12
Solution date: 2020-11-23
Public disclosure: 2021-04-30
CVE reference: CVE-2020-28943
CVSS: 7.7 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N)

Vulnerability Details:
Snippets are used to temporarily store content for internal handling, for example when using mail signatures or
E-Mail attachments while moving them to Drive ("managed files"). The identifier of those snippets could be
defined via an API call and are being used as reference when retrieving the file from any of the caches. When
timing this retrieval correctly and waiting for cache eviction and garbage collection, those snippets could be
used to reference arbitrary network resources instead of a snippet content while moving the snipped back from
the distributed to the local cache. Path traversal techniques could be used to escape the predefined valid URI
for those snippets.

Risk:
Arbitrary network resources could be requested by a malicious user through the middleware, including those
resources within a internal trust boundary where OX App Suite middleware operates. In case of web services,
this could expose the response of the service to the user. Services that use authentication or do not respond
to GET requests are not affected.

Steps to reproduce:
1. Create a snippet (e.g. image attachment) and use a malicious identifier
2. Wait for a couple of minutes until the snippet expires from the local map
3. Request the snippet to force it being requested from the distributed map and use the malicious reference

Solution:
We now use URI encoding when retrieving distributed managed files to avoid the ability to request resources out
of scope for the application. Independent from this, we suggest operators to use existing Security Manager
configuration to restrict network access of the middleware process to a reasonable scope.



---



Affected product: OX Guard
Internal reference: GUARD-228
Vulnerability type: Denial Of Service (CWE-400)
Vulnerable version: 2.10.4 and earlier
Vulnerable component: guard
Report confidence: Confirmed
Solution status: Fixed by Vendor
Fixed version: 2.10.3-rev8, 2.10.4-rev5
Vendor notification: 2020-11-02
Solution date: 2020-11-23
Public disclosure: 2021-04-30
CVE reference: CVE-2020-28944
CVSS: 3.1 (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L)

Vulnerability Details:
WKS is being used as an option to retrieve a users public key material for encrypted mail communication. In
case an attacker would setup malicious WKS infrastrucutre, OX Guard can be tricked to keep connections open for
a long period of time or process unusually large chunks of data.

Risk:
OX Guard nodes could be forced to exhaust system resources like network sockets, memory and connection pools.
This would lead to temporary unavailability of the service.

Steps to reproduce:
1. Setup a malicious WKS service, that responds very slowly and/or with huge amounts of data
2. Add one or more E-Mail recipient in OX App Suite which domain is handled by this malicious WKS service

Solution:
We added timeouts for both size and total connection duration to avoid being stuck processing responses from
malicious sources.
```

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

Login or Register to add favorites