ObjectPlanet Opinio 7.12 Cross Site Scripting

Authored by Ang Kar Min | Posted Jul 29, 2021

ObjectPlanet Opinio version 7.12 suffers from reflective and persistent cross site scripting vulnerabilities.

tags | exploit, vulnerability, xss
advisories | CVE-2020-26563
SHA-256 | f500e5fdb33867b5edf3170e3933efe781565d176bbb6a77f75941889807d9d6 Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title: ObjectPlanet Opinio 7.12 allows Cross-Site Scripting
# Vendor Homepage: https://www.objectplanet.com/opinio/
# Software Link: https://www.objectplanet.com/opinio/
# Exploit Authors: Ang Kar Min (https://www.linkedin.com/in/karmin-ang)
# CVE: CVE-2020-26563

# Timeline
- September 2019:  Initial discovery
- July 2020:  Reported to ObjectPlanet
- August 2020:  Fix/patch provided by ObjectPlanet
- July 2021:  Published CVE-2020-26563

# 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 is vulnerable to stored Cross-Site Scripting (Stored XSS) and reflected
Cross-Site Scripting (Reflected XSS).

# 3. Proof of Concept

### Reflected XSS executed in URL ###

The following payload was executed when injected as part of the URL"/survey/admin/surveyAdmin.do?
action=viewSurveyAdmin&surveyId=1234":

"&zwzc4%22%3e%3cinput%20type%3dtext%20autofocus%20onfocus%3dconfirm(1)%2f%2f"

Affected URL:/survey/admin/surveyAdmin.do?


### Stored XSS ###
Stored XSS payload such as "<script>alert('XSS ATTACK')</script> can be saved for various parameter fields.
This malicious payload can be executed upon a user visit to a page that publishes or previews the payload.

For example, a malicious XSS script can be added during the creation of a survey question for a given survey.
During the preview of the survey, the stored XSS payload will trigger the XSS vulnerability.

The previous example can be observed in other variations of the vulnerability where the affected parameters
accepts the malicious script.

Affected URL(s) and Parameter(s):
- /survey/admin/question.do
'questionText', 'ratingMinText', 'ratingMaxText', 'ratingNALabel', 'multMinError', 'numError', 'numPrefix',
'numPostfix', 'numReqError', 'dropdownLabel',  parameters

- /survey/admin/section.do
'title' parameter

- /survey/admin/sectionText.do
'text' parameter

- /survey/admin/plugin.do
'plugin_survey_closed_message', 'plugin_restrict_nrics', '&plugin_survey_email_content' parameter

- /survey/admin/confirm.do
'confirmMessageKeyParam', 'org.apache.struts.taglib.html.TOKEN' parameter

- /survey/admin/folder.do
'msgKey' parameter

- /survey/admin/file.do
'resourceName', 'resourcePath' parameter

- /survey/admin/setup.do
'characterEncoding', 'emailForErrors', 'fromEmail', 'language', 'systemBaseUrl' parameters

- /survey/admin/questionList.do?action=viewQuestionList&surveyId=1806
arbitrarily supplied URL parameter

- /survey/admin/resources.do?
action=viewResourcesByType&resourceType=8&fileListType=6125&selectedPreviewLocation=&selectedPreviewHeight=&sel
arbitrarily supplied URL parameter

- /survey/admin/surveyAdmin.do?action=viewSurveyAdmin&surveyId=3404&isPoll=1
arbitrarily supplied URL parameter


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

# 5. Credits
Ang Kar Min (https://www.linkedin.com/in/karmin-ang)
```

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

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