ObjectPlanet Opinio 7.13 Shell Upload

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

Posted Jul 30, 2021

ObjectPlanet Opinio version 7.13 suffers from a remote shell upload vulnerability.

tags | exploit, remote, shell
advisories | CVE-2020-26806
SHA-256 | 6146594a8eedc5b48c3895039ed9ff9b2da349396d6a84e9003398290c0214e6 **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-2020-26806

# Exploit Title: ObjectPlanet Opinio version 7.13 allows unrestricted file upload
# 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-2020-26806

# Timeline
- September 2020:  Initial discovery
- October 2020:  Reported to ObjectPlanet
- November 2020:  Fix/patch provided by ObjectPlanet
- July 2021:  CVE-2020-26806

# 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 unrestricted file uploads

# 3. Proof of Concept

### Unrestricted File Upload leading to RCE ###

Step 1:

URL: /opinio/admin/file.do

Opinio allows an administrative user to edit local CSS files. This file editing function however does not
validate if the HTTP POST parameters are tampered with.

Post parameters to tamper with:
- filePath
- fileContent

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.

The file path can be tampered with for e.g. : /upload/css/common/../../../admin/shell.jsp
The fileContent value was tampered with a JSP webshell for this PoC and a webshell was acheieved
For our PoC, we could view the web.xml file using an XXE vulnerability CVE-2020-26564 and identify which JSP
files were allowed be loaded and replaced the contents of that JSP file with the webshell code

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