Security Research Advisory

Abiquo Cloud

Path Traversal Vulnerability

Table of Contents

Path Traversal					Advisory Number
					SN-10-07
Severity	Software	Version(s)	Accessibility	CVE	Author(s)
H	Abiquo Cloud Community Edition	1.5 1.0	Remote	-	Claudio Criscione
	Vendor URL		Advisory URL		
	http://www.abiquo.com		-		

Date	Details
08/06/2010	Vendor disclosure
n./d.	Vendor acknowledgment
n./d.	Patch release
n./d.	Public disclosure

Summary

From the product's web page: "Designed from the ground-up to provide next generation Cloud management, Abiquo is the most complete and advanced solution available on the market today. Abiquo not only provides class-leading features like virtual to virtual conversion, it is easy to implement and operate, liberating your IT organization from the drudgery of managing thousands of virtual machines, without relinquishing control of the physical infrastructure."

Multiple pre-authentication remote path traversal vulnerabilities were identified in Abiquo's REST management interface.

Vulnerability Details

Abiquo's REST management interface provides a rich set of APIs to manipulate virtual machines or the whole datacenter. The REST interface does not implement any specific authentication for some functions, failing to properly validate user's input.

Technical Details

Description

The issue can be exploited with any web browser by issuing the following request to the REST endpoint.

PoC Request:

```
/am/rest_AM/downloadFileFromPath/?imagePath=../../../../../../../../../../../../etc/passwd
```

A VASTO module has been developed to exploit the issue.

Legal Notices

Secure Network (www.securenetwork.it) is an information security company, which provides consulting and training services, and engages in security research and development.

We are committed to open, full disclosure of vulnerabilities, cooperating with software developers for properly handling disclosure issues.

The information in the advisory is believed to be accurate at the time of publishing based on currently available information. This information is provided as-is, as a free service to the community by Secure Network research staff. There are no warranties with regard to this information. Secure Network does not accept any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.

If you have any comments or inquiries, or any issue with what is reported in this advisory, please inform us as soon as possible.

e-mail	info@securenetwork.it
phone	+39 02 917 730 41