

# [NEWS] Checkpoint FW1 SecuRemote/SecureClient "re-authentication" (client side hacks of users.C)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-03/0065.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 03/13/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Wed, 13 Mar 2002 10:33:33 +0100 (CET)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

-----

Checkpoint FW1 SecuRemote/SecureClient "re-authentication" (client side hacks of users.C)

---

## SUMMARY

Checkpoint Firewall-1 SecuRemote/SecureClient "authentication timeout" defined in FW1's security policy can be trivially bypassed at the client side.

## DETAILS

Vulnerable systems:

All versions of Checkpoint FW1 when used with SecuRemote/SecureClient (Namely 4.0, 4.1 at any SP level, and NG FP1):

<[http://www.checkpoint.com/products/security/vpn-1\\_clients.html](http://www.checkpoint.com/products/security/vpn-1_clients.html)>

[http://www.checkpoint.com/products/security/vpn-1\\_clients.html](http://www.checkpoint.com/products/security/vpn-1_clients.html)

When using Checkpoint FW1 together with Remote Users connected thru SecuRemote and SecureClient (

<[http://www.checkpoint.com/techsupport/downloads\\_sr.html](http://www.checkpoint.com/techsupport/downloads_sr.html)>

[http://www.checkpoint.com/techsupport/downloads\\_sr.html](http://www.checkpoint.com/techsupport/downloads_sr.html)), firewall administrators have the option of making these remote users

## Securiteam: [NEWS] Checkpoint FW1 SecuRemote/SecureClient "re-authentication" (client side hacks of users.C)

re-authenticate after X minutes.

This can be found in FW1's GUI inside :  
Global Properties -> Desktop Security -> Validation timeout

This feature is described in the help file as:  
Validation timeout every...minutes  
If checked, users must re-authenticate after the specified time.

However, this setting can be trivially bypassed by modifying the client side, inside SecuRemote's "users.C" configuration file.  
(You receive this file when first authenticating. It doesn't change until you "update" the site. Users.C also contains the encryption domain, and a lot of other stuff to play with, see references.)

Values to modify are "to\_expire (true)" and/or "expire (60)".

Replacing "true" by "false" will make your connection permanent, (no need to re authenticate whatever your Firewall admin wants). Changing the expire timeout (in minutes) to your liking can be used as well.

Nothing in the docs warns about this behavior.

This behavior was discovered under FW1 4.0, and was still working with 4.1 (any service pack) and is still working with FW1-NG FP1. Earlier versions are probably affected as well.

There are probably plenty of others settings that can be played with inside users.C, modifying DNS, encryption domains & networks is know to work, tough it leads to nothing useful if your security policy is solid. This advisory should be considered as a "proof of concept" on client-side users.C hacks.

### Impact:

Low. But if you actually use this feature inside your company and think it's doing anything useful about your security: you're wrong.

### Vendor Response:

This email is in response to the issue you have raised with the re-authentication handling in VPN-1 SecuRemote and SecureClient.

First off, thank you for sending this email to Check Point, we appreciate the ability to respond to possible security concerns in a low key, deliberative manner.

WRT the issue at hand: generally speaking, yes, the re-authentication mechanism can be manipulated on the client side to reduce the need for re-entering credentials, overriding the management station settings. To accomplish this several things must be in place:

1 - the user must be an authorized user (i.e., has a SR

[NEWS] Checkpoint FW1 SecuRemote/SecureClient "re-authentication" (client side hacks of users.C)

Securiteam: [NEWS] Checkpoint FW1 SecuRemote/SecureClient "re-authentication" (client side hacks of users.C)

username/authentication credentials)

2 – the user must be using "cacheable" credentials, such as: pre-shared secret, OS password or FW-1 internal passwords

3 – the user must be able to edit the users.C file

4 – the user must have some hostile intent or is very uneducated in security practices (like posting their credentials on their keyboard) or their machine has been compromised.

Several mechanisms exist to mitigate the above:

– As of NG, the users.C file does not need to be writeable by non-administrator privileged users. For bounded OSES like NT, 2000, and XP this solves the issue, unless the user has administrative privileges.

– Using a one time (S/Key) or periodic-based authentication credential (SecurID)

– The encrypt\_db (available in 4.0, 4.1 and NG) feature allows FW-1 administrators to, in effect, hide the topology data within users.C where these settings are located. The encrypt\_db property is NOT overridable by the client (i.e., even if they change the setting of obscure\_db in users.C they must delete/re-create the site to get in clear). Clearly, this is a security-through-obscurity mechanism and is not perfect.

– As of 4.1, one can force topology data to be updated automatically and frequently, forcing the user to modify these re-authentication settings in the users.C after each update (these are override-able, but can be obscured as well).

In summary, although yes, in theory you can override the re-authentication timer, it does require someone with authorized credentials (or a compromised machine with those credentials available). And, there are ways to manage/mitigate this.

We will also look at steps to add some mechanisms to enforce this, but again, for platforms like WinCE, and 9X this is problematic due to the lack of a privileged (super)user mechanism inherent in these OSES.

Thank you again for your communication on this matter.

#### ADDITIONAL INFORMATION

This vulnerability was discovered by Amaury de Ville & <mailto:cedric@cedric.net> Cedric Amand.

#### References:

A previous analysis of "users.C" inside "pen-test":  
<<http://lists.jammed.com/pen-test/2001/05/0040.html>>  
<http://lists.jammed.com/pen-test/2001/05/0040.html>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)

[NEWS] Checkpoint FW1 SecuRemote/SecureClient "re-authentication" (client side hacks of users.C)

Securiteam: [NEWS] Checkpoint FW1 SecuRemote/SecureClient "re-authentication" (client side hacks of users.C)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====  
=====

**DISCLAIMER:**

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

- 
- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[NEWS] mIRC DCC Server Security Flaw"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)