

Check Point
SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.

FireWall-1 HTTP Security Server Hotfix

Posted: February 4, 2004
Updated: February 6, 2004



Intelligent Security



A vulnerability in the FireWall-1 HTTP Security Servers exists that may cause it to crash in certain circumstances, which is very difficult to manipulate but might allow further exploitation. This issue only exists when using HTTP Security Servers.

In order to protect FireWall-1 against this vulnerability, Check Point recommends that customers apply a simple change to a configuration file on the enforcement modules that will solve the problem.

Affected Releases:

VPN-1/FireWall-1 NG and above, only when using HTTP Security Servers.
VPN-1/FireWall-1 4.1 (all Service Packs) **are NOT** affected.

If the HTTP Security Servers are not in use on the module, there is no need to install the update.

The update is applicable on the following releases:

1. NG FP3 HF2
2. NG with Application Intelligence R54
3. NG with Application Intelligence R55
4. Other NG based releases (NG FCS, NG FP1, NG FP2)

Instructions:

In order to fix the potential security vulnerability, one of the following courses of action should be taken on each FireWall-1 module. In cluster environments, perform the actions on the standby member first, fail over to it, and then perform them on the member that was active.

1. In most deployments, the `cpsec.conf` file, located in `$FWDIR/lib/` and `cpsec.en_us` file, located in `$FWDIR/conf/cpsec/` have not been manually adjusted. Apply the update by replacing the `cpsec.en_us` and `cpsec.conf` with the new version as follows:
 - a. Download the new `cpsec.conf` file from Check Point
 - b. Create a backup of `$FWDIR/conf/cpsec/cpsec.en_us`
 - c. Copy and rename the new `cpsec.conf` file to `$FWDIR/conf/cpsec/cpsec.en_us`
Note: If you are using non-English language, replace the `cpsec.XXX` file appropriate for your language.
 - d. In addition, copy the new `cpsec.conf` file to `$FWDIR/lib/cpsec.conf`, overwriting the old `cpsec.conf` file
 - e. Activate the change by running "fw kill fwd" to restart the fwd
2. If the `cpsec.en_us` file (located in `$FWDIR/conf/cpsec/`) has been manually changed, and the customer does not wish to override the changes, the following steps should be taken:
 - a. Edit the `$FWDIR/conf/cpsec/cpsec.en_us` file
Note: If you are using non-English language, replace the `cpsec.XXX` file appropriate for your language.
 - b. Search inside the file for the label "CPSEC_HTTP_SCHEME_NOT_SUPPORTED" and remove the string "#.50scheme#" from the adjacent string.
For example, replace the line

```
CPSEC_HTTP_SCHEME_NOT_SUPPORTED 1024 "Scheme #.50scheme# not supported by http daemon"
```

with the line

```
CPSEC_HTTP_SCHEME_NOT_SUPPORTED 1024 "Scheme not supported by http daemon"
```



- c. Search inside the file for the label "CPSC_HTTP_FW_UNAUTH" and remove the string "#.50user#" from the adjacent string.

For example, replace the line

```
CPSC_HTTP_FW_UNAUTH          1024  "\n\n#local_host# Unauthorized to
access the document.<BR><BR><LI>Authorization is needed for FW-
1#.100realm#. <BR><BR><LI>The authentication required by FW-1 for #.50user# is:
<STRONG>#.30auth_prompt#</STRONG>.<BR><BR><LI>#reason_title#:
<STRONG>#.100reason#</STRONG>#.199new_loc#\n" (local_host realm user
auth_prompt reason_title reason new_loc)
```

with the line

```
CPSC_HTTP_FW_UNAUTH          1024  "\n\n#local_host# Unauthorized to
access the document.<BR><BR><LI>Authorization is needed for FW-
1#.100realm#. <BR><BR><LI>The authentication required by FW-1 is:
<STRONG>#.30auth_prompt#</STRONG>.<BR><BR><LI>#reason_title#:
<STRONG>#.100reason#</STRONG>#.199new_loc#\n" (local_host realm user
auth_prompt reason_title reason new_loc)
```

- d. Search inside the file for the label "CPSC_HTTP_UNKNOWN_SCHEME_ERR" and remove the string "#.40scheme#" from the adjacent string.

For example, replace the line

```
CPSC_HTTP_UNKNOWN_SCHEME_ERR 1024  "\n\n#local_host# Scheme
<STRONG>#.40scheme#</STRONG> not supported." (local_host scheme)
```

with the line

```
CPSC_HTTP_UNKNOWN_SCHEME_ERR 1024  "\n\n#local_host# Scheme
not supported." (local_host scheme)
```

- e. Save the file
 f. The same changes (steps 2a-2e) should also be applied to the cpsc.conf in \$FWDIR/lib
 g. In order to activate the change, restart the fwd by running "fw kill fwd"