



We Secure the Internet.

Connectra 2.0 Security Hotfix 2 Release Notes

October 5, 2006



Introduction

Connectra 2.0 Security Hotfix 2 resolves a security vulnerability described at http://www.openssl.org/news/secadv_20060928.txt that relates to the OpenSSL SSL/TLS library (libssl). This library is used by Connectra, so that installing this hotfix is strongly recommended.

This hotfix includes all previous Connectra security hotfixes.

The latest version of this document is available for download from:
<http://www.checkpoint.com/downloads/latest/hfa/connectra.html>.

In This Document

<i>Resolved Limitations</i>	<i>page 2</i>
<i>Installation Instructions</i>	<i>page 3</i>
<i>Installation Instructions</i>	<i>page 3</i>

Resolved Limitations

Resolved in this Security Hotfix

Recent OpenSSL advisories reveal vulnerabilities in OpenSSL which may allow a malicious user to perpetrate a Denial of Service attack. Connectra uses the OpenSSL SSL/TLS library (libssl) and may therefore be affected. For more information, see http://www.openssl.org/news/secadv_20060928.txt.

Also Resolved in Previous Security Hotfixes

Recent OpenSSL advisories reveal vulnerabilities in OpenSSL which may allow forged certificates to be verified as correct. Connectra uses the OpenSSL SSL/TLS library (libssl) and may therefore be affected. For more information, see http://www.openssl.org/news/secadv_20060905.txt.

Installation Instructions

Connectra 2.0 Security Hotfix can only be installed over the following:

- Version 2.0 Hotfix Accumalator (HFA_1)
- Previous Connectra security hotfixes.

It is installed using the command line. Before installing, it is recommended to preserve the previous configuration by taking a snapshot image.

In This Section

Preserving the Previous Configuration	page 3
Installation	page 4
Reverting to a Previous Version	page 5

Preserving the Previous Configuration

Before installing the Hotfix, it is recommended that you create an image of the entire system using the `snapshot` tool, either locally or on a TFTP or SCP server. This feature greatly reduces the risks of configuration changes.

With a `snapshot` image you can restore the installation to the state before the upgrade, using the `revert` command. At boot time you are given the option of booting from any of the available snapshots.

To make it possible to uninstall this Hotfix, create a `snapshot` image before installation. You can then uninstall using the `revert` command.

Running the `snapshot` command without any additional flags runs it in interactive mode that takes you through the process.

You can also create a snapshot image using the command line syntax.

Snapshot Command Syntax

```
snapshot [-h] [-d] [--tftp <ServerIP> <Filename>]
          | [--scp <ServerIP> <Username> <Password> <Filename>]
          | [--file <Filename>]]
```

TABLE 1-1 Snapshot command parameters

Parameter	meaning
-h	Obtain usage.
-d	Generate debug information.
--tftp <ServerIP> <Filename>	IP address and TFTP server from which the snapshot is made as well as the snapshot's filename.
--scp <ServerIP> <Username> <Password> <Filename>	IP address of SCP server from which the snapshot is made, the username and password used to access the SCP Server, and the filename of the snapshot.
--file <Filename>	When the snapshot is made locally, specify a filename.

Installation

- 1 Download the Connectra 2.0 security hotfix 2 package from the Check Point Download Center <https://downloads.checkpoint.com/dc/login.htm>.
- 2 Open an SSH connection to Connectra, or connect to it via a console.
- 3 Log in to Connectra using your administrator username and password.
- 4 Change to Expert mode by typing `expert` and supplying the password.
- 5 Use FTP in bin mode to upload the package to Connectra to a temporary directory.
- 6 Backup files to be replaced in the Hotfix by running the following command:

```
gtar -cf ssl_hf_backup.tar $CVPNDIR/bin/openssl $CVPNDIR/lib/*.9.7
```

A file name `ssl_hf_backup.tar` will be created in your current directory, which includes the files that will be replaced by the Hotfix. Save this file to a secure location to enable uninstall of the Hotfix.

- 7 Stop all Check Point processes by running `cpstop`.
- 8 Open the `tgz` package by running the following command:

```
gtar -zxpvf ssl_HOTFIX2_2.0.tgz
```

-
- 9 Copy the new files to the required locations by running the following commands from the temporary directory to which you extracted the files:

```
cp lib*.0.9.7 $CVPNDIR/lib/
cp openssl $CVPNDIR/bin/
```

- 10 After the installation is complete, run `cpstart` to start Check Point processes.

Reverting to a Previous Version

Using the Revert Command

If a SecurePlatform snapshot was created before the installation as recommended, reverting to the pre-security Hotfix state can be done using the `revert` command.

Running the `revert` command without any additional flags runs it in interactive mode that takes you through the process of restoring the machine.

You can also use the command line syntax.

The `revert` command functionality can also be accessed from the **Snapshot image management** boot option of Connectra.

Syntax

```
revert [-h] [-d] [[--tftp <ServerIP> <Filename>]
                | [--scp <ServerIP> <Username> <Password> <Filename>]
                | [--file <Filename>]]
```

TABLE 1-2 Revert command parameters

Parameter	meaning
-h	Obtain usage
-d	Generate debug information
--tftp <ServerIP> <Filename>	IP address and TFTP server from which the snapshot is rebooted, as well as the filename of the snapshot.
--scp <ServerIP> <Username> <Password> <Filename>	IP address of SCP server from which the snapshot is rebooted, the username and password used to access the SCP Server, and the filename of the snapshot.
--file <Filename>	When the snapshot is made locally, specify a filename.

Reverting from a Backup File

Reverting the machine to the pre-Hotfix installation state can be done using the backup file (`ssl_hf_backup.tar`) created in [step 6](#) of the “[Installation](#)” section.

- 1 Stop all Check Point processes by running `cpstop`.

-
- 2** Open the `tgz` package by running the following command:

```
gtar -zxpvf ssl_hf_backup.tar
```

- 3** Copy the new files to the required locations by running the following commands from the temporary directory to which you extracted the files:

```
cp lib*.0.9.7 $CVPNDIR/lib/
```

```
cp openssl $CVPNDIR/bin/
```

- 4** After the installation is complete, run `cpstart` to start Check Point processes.