OpenSSL Hotfix for 4.1 SP6
August 2002

1   Overview

This Hotfix addresses a security alert published regarding OpenSSL: CERT® Advisory CA-2002-23 "Multiple Vulnerabilities In OpenSSL".
The issues which concern Check Point's use of OpenSSL are also being referenced as Common Vulnerabilities and Exposures project references: CAN-2002-0656, CAN-2002-0659
The Hotfix addresses the resulting vulnerabilities, mainly originating from possible buffer overruns in the OpenSSL code.

2   Relevant versions

This Hotfix is relevant only for 4.1 SP6

3   Supported Platforms

This hot-fix is available for the following platforms:
- Solaris
- Windows
- Linux
- HPUX
- AIX
- IPSO

4   Installation

This Hotfix requires a replacement of files depending on specific deployment configurations.

4.1   *Enforcement module/ Management Server*

To apply this fix to the enforcement module – proceed as follows:

4.1.1   Windows

1. Download
   a. WIN32: openssl_HF_41_SP6_B41623_win32_[encryption].tgz
   b. W2K: openssl_HF_41_SP6_B41623_win2k_[encryption].tgz

   to a temporary directory and extract the files to a temporary directory.
2. Using a command-line run the following commands:
   'fwstop'
3. If ELA Proxy is running - stop ELA Proxy by running the following command using the command-line:
   'net stop elaservice'
4. replace fw.exe under %FWDIR%\bin

5. replace ela_proxy.exe under %FWDIR%\bin
6. Using a command-line run the following commands:
    a. 'fwstart'

7. To restart ELA Proxy - using the command-line run the command:
    'net start elaservice'

8. To verify that the fix is applied, open a command line window:
    a. Change directory to %FWDIR%
    b. Run 'fw ver' and make sure that the Build Number field is the correct one: 41623

4.1.2 Unix Platforms

1. Download
    a. Solaris: openssl_HF_41_SP6_B41623_solaris2_[encryption].tgz
    b. Solaris-i386:
        openssl_HF_41_SP6_B41623_solaris2i386_[encryption].tgz
c. Linux: openssl_HF_41_SP6_B41623_linux_[encryption].tgz
    d. IPSO: openssl_HF_41_SP6_B41623_ipso_[encryption].tgz
    e. AIX: openssl_HF_41_SP6_B41623_aix_[encryption].tgz
f. HPUX: openssl_HF_41_SP6_B41623_hpux_[encryption].tgz
    to a temporary directory and extract the file to a temporary directory.
2. Run the following commands
        'fwstop'

3. If ELA Proxy is running - stop ELA Proxy by running the following command using the command:
        'elaproxyService -stop'

4. replace fw under $FWDIR/bin
5. replace ela_proxy under $FWDIR/bin
6. Run the following commands
        'fwstart'

7. To restart ELA Proxy - using the command-line run the command:
        'elaproxyService -start'

8. To verify that the fix is applied, open a command-line window:
    a. Change directory to $FWDIR
    b. Run 'fw ver' and make sure that the Build Number field is the correct one: 41623