



version of EOS, eAPI can be temporarily disabled.

**Verification:**

To determine if the version of EOS is vulnerable use the following steps. Access the bash prompt:

```
switch# bash
-bash-4.1#
```

Copy and paste the following script:

```
echo | timeout 3 openssl s_client -connect 127.0.0.1:443 >/dev/null 2>&1; if [[ $? != 0 ]]; then echo "UNKNOWN: 127.0.0.1 timeout or connection error"; else echo | openssl s_client -connect 127.0.0.1:443 -ssl3 2>&1 | grep -qo "ssl3 alert handshake failure" && echo "OK: 127.0.0.1 Not vulnerable" || echo "FAIL: 127.0.0.1 vulnerable; ssl3 connection accepted"; fi
```

If the output of the above command contains

```
"OK: 127.0.0.1 Not vulnerable"
```

then your system is not vulnerable.

If the output of the above command contains

```
"FAIL: 127.0.0.1 vulnerable; ssl3 connection accepted"
```

then your system is vulnerable.

If you receive

```
"UNKNOWN: 127.0.0.1 timeout or connection error"
```

then eAPI is not running or is running on a non-default port. If eAPI is running with a non-default port number modify the script replacing 443 with the port number in use.

**Resolution:**

The resolution to this issue is through upgrading to a version of EOS that already contains the resolution or through the installation of a patch.

Download URL for patch: [secAdvisory0007.swix](#)

**Instructions to install the patch for Security Advisory 0007**

The extension is applicable for EOS versions 4.12.0 - 4.12.7.1, 4.13.0 - 4.13.6 inclusive.

Step 1. Copy the file secAdvisory0007.swix to the extension partition of the Arista switch using any of the supported file transfer protocols:

```
switch#copy scp://arista@10.10.10.123/home/arista/secAdvisory0007.swix
extension:
```

Step 2. Ensure that the file has been copied to the extensions partition and verify the checksum of the copied file:

```
switch#show extensions
Name                Version/Release      Status<          RPMs
-----
secAdvisory0007.swix secAdvisory0007.swix 1.0.0/2122170.cohud
sondev              A, NI                1
A: available | NA: not available | I: installed | NI: not installed |
F:forced
```

To verify the extension, compare the following sha512 or md5 checksum with the output of the verify command:

```
sha512sum:
59d3eac06ad9670b94431d569e100165d6d831c0c92dbe72130db7ab81b24e25a68c2a
f277de5386724405dd9d79e168c9156b4cc6a532fecabf18caf7548160
```

```
md5sum:
3cca393084e6d51e794f04d65f23c389
```

**verify commands:**

```
switch#verify /sha512 extension:secAdvisory0007.swix
verify /sha512 (extension:secAdvisory0007.swix) = 59d3eac06ad9670b9443
1d569e100165d6d831c0c92dbe72130db7ab81b24e25a68c2af277de5386724405dd9d
79e168c9156b4cc6a532fecabf18caf7548160
```

```
switch#verify /md5 extension:secAdvisory0007.swix
verify /md5 (extension:secAdvisory0007.swix) =
3cca393084e6d51e794f04d65f23c389
```

Step 3. The patch is installed as an extension, and upon installation into a live system will automatically install with the following behavior:

```
switch#extension secAdvisory0007.swix
```

All modular switches with dual supervisors require the extension copying and installing on both supervisors.

Verify that the extension has been installed:

```
switch#show extensions
Name                Version/Release          Status          RPMs
-----
secAdvisory0007.swix 1.0.0/2122170.cohudsondev A, I 2

A: available | NA: not available | I: installed | NI: not installed |
F: forced
```

Step 4. Post installation, eAPI will be restarted and will be unavailable for a few seconds, and all existing connections will be dropped.

Step 5. Make the extension persist across reboots:

```
switch#copy installed-extensions boot-extensions
```



If you require further assistance, or if you have any further questions regarding this security notice, please contact the Arista Networks Technical Assistance Center (TAC) by one of the following methods:

Open a Service Request:

By email: [support@arista.com](mailto:support@arista.com)

By telephone: 408-547-5502

866-476-0000