Date: October 17th, 2016

Version: 1.1

Revision	Date	Changes
1.0	October 17th, 2016	Initial Release
1.1	October 18th, 2016	Affected platforms section is expanded

Affected Platforms: **DCS-7050 series** only - 7050S, 7050T, 7050Q platforms (7050X series of products is not affected). None of the other platform families are affected.

Affected Software Version: All EOS releases after EOS-4.15.2F

CVE-2016-6894

CVSS v2 Base Score: 7.8 (High)

Impact: This advisory is to document a security vulnerability that affects Arista products. On the DCS-7050 series, sending certain packets to the control plane can cause the device to unexpectedly reboot.

After the switch reload, "show reload cause" will have a backtrace with the following line that is indicative of this vulnerability.

[2330.476815] strata-dma: sobmh_ts_offset_set::unsupported sobmh version=0x5
[2330.752624] ------------[cut here]------------
[2330.754711] kernel BUG at /usr/include/CpuFabric/strata-dcb.h:509!

BUG158250 tracks this vulnerability. A fix for this issue is available in versions 4.15.8M, 4.16.7M, 4.17.0F.

Resolution: It is recommended to upgrade EOS to versions with the fix (4.15.8M, 4.16.7M or 4.17.0F) or install the patch provided on affected versions of EOS.

Patch file download URL: CVE-2016-6894-hotfix.swix

Sha256 sum is:

[admin@switch flash]$ sha256sum CVE-2016-6894-hotfix.swix
bc7c2f2906e04bff71df5ba8d10bdf03c0773b3dc40b97726060d6dab972def9
CVE-2016-6894-hotfix.swix

Note:

- This hotfix can be installed on all affected versions of EOS.
- Installing the patch will restart the forwarding agent that could lead to a momentary disruption in traffic forwarding.
- A reload of the switch is not required for the patch to take effect

Instructions to install the patch

1. Download the patch file and copy the file to the extension partition of the switch using one of the supported file transfer protocols:

```
switch#copy scp://10.10.0.1/CVE-2016-6894-hotfix.swix extension:
switch#verify /sha256 extension:CVE-2016-6894-hotfix.swix
```

   Verify that the checksum value returned by the above command matches the provided SHA256 checksum for the file
2. Install the patch using the extension command. The patch takes effect immediately at the time of installation.

```
switch#extension CVE-2016-6894-hotfix.swix
```

3. Verify that the patch is installed using the following commands:

```
switch#show extensions
Name                                      Version/Release           Status ex
tension
----------------------------------------- ------------------------- ------ --
--
CVE-2016-6894-hotfix.swix                 2.7.0/3450908.idcaldwellS A, I
 1
A: available | NA: not available | I: installed | NI: not installed | F: force
d
```

4. Make the patch persistent across reloads. This ensures that the patch is installed as part of the boot-sequence. The patch will not install on EOS versions with the security fix.

```
switch#copy installed-extensions boot-extensions
switch#show boot-extensions
CVE-2016-6894-hotfix.swix
```

References:

CVE-2016-6894

Open a Service Request:

By email: support@arista.com
By telephone: 408-547-5502
866-476-0000