Date: November 18th, 2015

Revision	Date	Changes
1.0	November 18th, 2015	Public release
1.1	November 18th, 2015	Updated to include CVE number and bug ID

Arista EOS Remote Privilege Escalation Vulnerability - CVE-2015-8236

This advisory is to document a security vulnerability identified by Arista Networks that affects EOS. Affected EOS releases are listed in Table-1 below. This issue is a privilege escalation vulnerability that could allow a remote attacker with IP connectivity to the management plane of the switch to run arbitrary code as a privileged user. This includes getting root level access to the bash shell on the switch. It is not required for the attacker to have credentials for a user account on the switch. All methods of management plane access are exposed.

NOTE: This vulnerability was identified internally by Arista Networks and there have been no external reports of an exploit, as of the date of this notice.

Recommended Action: For switches running any affected EOS version, the immediate recommendation is to install a non-disruptive patch or to upgrade to a remediated version of EOS. Either step will prevent any exploit.

A single patch for this issue is available for EOS versions 4.5.0 and later via the URL below and this patch can be installed non-disruptively. Applying this patch serves as a permanent resolution to this issue. Instructions to install the patch is documented in this advisory.

Table-2 below contains the list of EOS versions that contain the security fix.

Affected software releases: All EOS releases shipped prior to the date of this release are affected. The following table only lists the affected EOS versions from the supported release trains. Release trains older than 4.11, such as 4.10, 4.9, 4.8, 4.7, 4.6, 4.5 and older, are affected as well.

4.15	4.14	4.13	4.12	Older release trains
4.15.0F • 4.15.0FX • 4.15.0FX A • 4.15.0FX	4.14.0F 4.14.1F 4.14.2F 4.14.3F 4.14.3.1F 4.14.4F 4.14.4.1F	4.13.1.1F 4.13.2.1F 4.13.3.1F 4.13.4.1F 4.13.5F 4.13.5.1F 4.13.6F	4.12.5.2 4.12.6.1 4.12.7.1 4.12.8 4.12.8.1 4.12.9 4.12.10	All releases in 4.11 All releases in 4.10 All releases in 4.9 All releases in

Copyright 2025 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

1 4.15.1F • 4.15.1FXB • 4.15.1FX-7060X • 4.15.1FX-7260QX 4.15.2F	4.14.4.2F 4.14.5F • 4.14.5FX • 4.14.5FX.1 • 4.14.5FX.2 • 4.14.5FX.3 • 4.14.5FX.4 • 4.14.5.1F-SSU 4.14.6M 4.14.7M 4.14.7.1M 4.14.8M 4.14.8.1M 4.14.9M	4.13.7M 4.13.7.2M 4.13.7.3M 4.13.8M 4.13.9M 4.13.9.1M 4.13.10M 4.13.11M 4.13.12M 4.13.13M		4.8 All releases in 4.7 All releases in 4.6 All releases in 4.5 All release trains older than 4.5

Table-1: Affected EOS releases

Affected platforms: All Arista platforms

Resolution: Bug 138716 tracks this vulnerability. The following table lists the releases that contain the fix for the vulnerability. These releases are available on the software downloads page.

EOS-4.15	EOS-4.14	EOS-4.13	EOS-4.12	EOS-4.11
4.15.0FX1.1 4.15.0FXA.1 4.15.1FXB.1 4.15.1FX-7060X.1 4.15.2.1F or later	4.14.5FX.5 4.14.5.1F-SSU.1 4.14.9.1M or later	4.13.14M or later	4.12.11 or later	4.11.12 or later

Table-2: EOS releases with security fix

Patch file download URL: secAdvisory0015.swix

MD5SUM: 12a669428dc3ac8697dffabed31c18f9

Copyright 2025 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

SHA512SUM: 4c98ba78dfa93f180e0f826d0d82f41219125dcccdf37595b65277193492fa9aa5ec13b79eec25765a8375b58d8594879e9d369175e9d6f9c3fd092392d0aee8

NOTE:

- The patch is applicable only to EOS versions starting at 4.5.0 and later
- Installing the patch is **non-disruptive** to switch operation or traffic flowing through the switch
- 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/secAdvisory0015.swix extension:
switch#verify /sha512 extension:secAdvisory0015.swix
```

   Verify that the checksum value returned by the above command matches the provided SHA512 checksum for the file
   On modular systems with dual supervisors, download the file to the extension partition of the active supervisor and copy it to the standby supervisor using the following two commands:

```
switch(s1)(config)#copy extension:secAdvisory0015.swix supervisor-
peer:/mnt/flash/
switch(s2-standby)#copy flash:secAdvisory0015.swix extension:
```

2. Install the patch using the extension command. The patch takes effect immediately at the time of installation.

```
switch#extension secAdvisory0015.swix
```

   On modular systems with dual supervisors, the patch has to be installed on the active and standby supervisors:

```
switch(s1)#extension secAdvisory0015.swix
switch(s2-standby)#extension secAdvisory0015.swix
```

   If eAPI is enabled, the eAPI agent or the uwsgi service will restart after the patch has been installed. One of following messages will be logged as a result:

```
ProcMgr-worker: %PROCMGR-6-PROCESS_RESTART: Restarting 'CapiApp' immediately
SuperServer: %SYS-4-RESTART_SERVICE: Service uwsgi is not running. Attempting
to restart it.
```

Copyright 2025 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

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

```
switch#show extensions
Name              Version/Release           Status extension
----------------- ------------------------- ------ ---------
secAdvisory0015.swix 1.0.0/SA15                A, I      1
A: available | NA: not available | I: installed
 | NI: not installed | F: forced
```

```
switch#show ver detail  | grep SA15
secAdvisory0015      1.0.0           SA15
```

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
secAdvisory0015.swix
```

For dual supervisor systems run the above copy command on both active and standby supervisors:

```
switch(s1)#copy installed-extensions boot-extensions
switch(s2-standby)#copy installed-extensions to boot-extensions
```

Instructions to uninstall the patch:

1. Uninstall the patch using the following command:

```
switch#no extension secAdvisory0015.swix
```

On modular systems with dual supervisors, the patch has to be uninstalled on the active and standby supervisors:

```
switch(s1)#no extension secAdvisory0015.swix
switch(s2-standby)#no extension secAdvisory0015.swix
```

The output of ‘show extensions’ will reflect the status of the patch as ‘NI: Not installed’

```
switch#show extension
Name              Version/Release           Status extension
```

Copyright 2025 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

```
---------------- ------------------------ ------ ---------
secAdvisory0015.swix 1.0.0/SA15               A, NI      1
A: available | NA: not avail
able | I: installed | NI: not installed | F: forced
```

NOTE: Once the extension has been uninstalled, the switch is no longer protected against the vulnerability.

2. To make this change persistent across switch reloads, run the following command to remove the patch from boot-extensions:

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

For dual supervisor systems run the above copy command on both active and standby supervisors:

```
switch(s1)#copy installed-extensions boot-extensions
switch(s2-standby)#copy installed-extensions boot-extensions
```

Upgrade considerations:

- It is recommended to uninstall the patch before upgrading to a remediated version of EOS. To uninstall the patch, follow the instructions above.
- When upgrading from EOS versions older than 4.11.0, please refer to the release notes for considerations around memory and software support

For More Information:
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
By telephone: 408-547-5502
866-476-0000

Copyright 2025 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.