Date: June 13th, 2016

Version: 1.0

Revision	Date	Changes
1.0	June 13th, 2016	Initial release

Arista Products vulnerability report for security vulnerability announcement from NGINX on May 31st, 2016

It was announced by NGINX on May 31, 2016 that there is a security update for NGINX. This advisory reports the vulnerability assessment for Arista products.

Vulnerability report for EOS and CVP:

EOS is **vulnerable** to the following:

CVE-2016-4450 (nginx security advisory):

Software versions	All EOS releases starting with 4.12.0F . The list of affected releases is documented in Table-2.
Status	Vulnerable
Affected Features	eAPI and Openstack
Details	A problem was identified in nginx code responsible for saving client request body to a temporary file. A specially crafted request might result in worker process crash due to a NULL pointer dereference while writing client request body to a temporary file.
Resolution	Bug 159252 tracks this vulnerability for EOS. A hotfix patch is available to address this issue. A software fix will be available in upcoming versions for the currently active EOS software trains. This advisory will be updated once the exact SW version is available.

Resolution

Copyright 2024 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.

Patch file download URL: secAdvisory0021.swix

sha512sum secAdvisory0021.swix

d7124b02ae8505436a94a0440b2c4192b801b30bd84ed1a9c3672c8c4891fadca18b6221237fb959436c5dd084e95bc97317606c41c6b173993becbc13c857e6 secAdvisory0021.swix

NOTE

- This hotfix can be installed on all affected versions of EOS.
- Installing the patch will temporarily disrupt nginx and eAPI sessions when applied
- 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/secAdvisory0021.swix extension:
switch#verify /sha512 extension:secAdvisory0021.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:secAdvisory0021.swix supervisor-peer:/mnt/flash/
switch(s2-standby)#copy flash:secAdvisory0021.swix extension:
```

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

```
switch#extension secAdvisory0021.swix
```

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

Copyright 2024 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.

```
switch(s1)#extension secAdvisory0021.swix
switch(s2-standby)#extension secAdvisory0021.swix
```

If eAPI is enabled, the eAPI agent or the uwsgi service will restart after the patch has been installed.

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

```
switch#show extensions
Name                                        Version/Release           S
tatus extension
------------------------------------------- ------------------------- -
----- ----
secAdvisory0021.swix                        1.6.2/3236644.idburleydev A
, I      1
A: available | NA: not available | I: installed | NI: not installed |
F: forced
```

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
secAdvisory0021.swix
```

5. 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
```

AFFECTED EOS RELEASES:

Table-2: Affected EOS releases

Copyright 2024 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.

4.16	4.15	4.14	4.13	Older release trains
4.16.6M	4.15.0F • 4.15.0FX • 4.15.0FXA • 4.15.0FX1 4.15.1F • 4.15.1FXB.1 • 4.15.1FXB • 4.15.1FX-7060X • 4.15.1FX-7060QX 4.15.2F 4.15.3F • 4.15.3FX-7050X-72Q • 4.15.3FX-7060X.1 • 4.15.3FX-7500E3 • 4.15.3FX-7500E3.3 4.15.4F • 4.15.4FX-7500E3 4.15.4.1F 4.15.5M • 4.15.5FX	4.14.0F 4.14.1F 4.14.2F 4.14.3F 4.14.3.1F 4.14.4.F 4.14.4.1F 4.14.4.2F 4.14.5M • 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 4.14.9.1M	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 4.13.7M 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 4.13.14M 4.13.15M	All releases in 4.12*

Copyright 2024 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.

	-7500R • 4.15.5FX -7500R-bgpscale 4.15.6M	4.14.10M 4.14.10.1M 4.14.11M 4.14.12M		
* First EOS release to support eAPI				

Vulnerability report for CloudVision Portal (CVP)

CloudVision Portal is only **affected** by the following vulnerabilities:

- **CVE-2016-4450** (nginx security advisory)

This is tracked by bug 159255 which will be fixed in release 2016.1.1.

References:

For more information on these vulnerabilities please visit:

http://mailman.nginx.org/pipermail/nginx-announce/2016/000179.html

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 2024 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.