Date: October 2nd, 2017

Version: 1.0

Revision	Date	Changes
1.0	October 2nd, 2017	Public release
1.1	October 3rd, 2017	Updates to clarify impact and add mitigation
1.2	October 6th, 2017	Updates to the affected software release table
1.3	October 11th, 2017	Hotfix v1.1 has been updated

A list of 6 CVEs affecting DNS and DHCP were publicly released on October 2nd, 2017 by the Google Security Research team. From internal investigations it has been confirmed that Arista Network's software products - EOS and Cloud Vision Portal (CVP) are not exploitable to the following DNS and DHCP vulnerabilities.

CVE-2017-14495: DNS - Lack of free () - OOM/DoS

CVE-2017-14496: DNS - Invalid boundary checks and integer underflow - DoS

CVE-2017-14492: DHCP - Heap based overflow - RCE

CVE-2017-14493: DHCP - Stack based overflow - RCE

CVE-2017-14494: DHCP - Information leak

This advisory documents the impact of CVE-2017-14491: DNS - 2 byte heap based overflow - RCE that affects some Arista Products.

CVSS v2 Score 10
CVSS v3 Score 9.8

This vulnerability could allow a remote attacker to run arbitrary code, create a denial of service or an out of memory situation.

- EOS - Affected versions of EOS (documented in Table-1) are vulnerable to CVE-2017-14491 when configured to use a DNS server using the command ‘ip name-server’ in the default as well as non-default VRFs.
- CloudVision Portal is not affected by CVE-2017-14491

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.

Note: There have been no external reports of an exploit, as of the date of this notice. Proof of concepts to evaluate if you are affected have been made available by the Google security research team that discovered the vulnerabilities.

Recommended Action: For switches running any affected EOS version with the 'ip name-server' configuration, 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. Removing the 'ip name-server' command from default and non-default VRFs will serve as mitigation against this vulnerability.

A single patch for this issue is available for EOS versions 4.13.0 and all later versions up to 4.19.0 via the URL below. This patch can be installed non-disruptively. Applying this patch serves as a permanent resolution to this issue. Instructions to install the patch are available on page 3 of this advisory.

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.

Table-1: Affected EOS releases

4.18	4.17	4.16	4.15	Older release trains
4.18.0F 4.18.1F • 4.18.1FX-7060X.2-SSU • 4.18.1FX-7060X.1-SSU • 4.18.1FX-7060X-SSU 4.18.1.1F 4.18.2F • 4.18.2-REV2-FX.1 • 4.18.2-R	4.17.0F 4.17.1F • 4.17.1FX-VRRP6LL 4.17.1.1F • 4.17.1.1FX-MDP 4.17.1.4F 4.17.2F • 4.17.2FX-OpenStack 4.17.2.1F	4.16.6M • 4.16.6FX-7500R • 4.16.6FX-7500R.1 • 4.16.6FX-7500R-bgpscale • 4.16.6FX-7512R • 4.16.6FX-7060X • 4.16.6FX-7050X2 • 4.16.6FX-7050X2.2 4.16.7M • 4.16.7FX	4.15.0F • 4.15.0FX • 4.15.0FX.1 • 4.15.0FXA • 4.15.0FXA.1 • 4.15.0FX1 • 4.15.0FX1.1 4.15.1F • 4.15.1FXB • 4.15.1FXB.1 • 4.15.1FX-7060X	All releases in 4.14 All releases in 4.13 Releases older than 4.13

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.

EV2-FX 4.18.2.1F 4.18.3F 4.18.3.1F 4.18.4F 4.18.4.1F 4.18.4.2F	4.17.3F • 4.17.3FX-7500R • 4.17.3FX-7500R.1 4.17.4M 4.17.5M 4.17.5.1M 4.17.6M 4.17.7M	-7500R • 4.16.7FX-7500R-bgpscale • 4.16.7FX-7500R-bgpscale.1 • 4.16.7FX-7060X • 4.16.7FX-7060X.1 • 4.16.7M-L2EVPN • 4.16.7FX-MLAGISSU-TWO-STEP • 4.16.7.1FX-ECMP-FIX 4.16.8M • 4.16.8FX-7500R • 4.16.8FX-7060X • 4.16.8FX-MLAGISSU-TWO-STEP 4.16.9M • 4.16.9FX-7500R • 4.16.9FX-7060X • 4.16.9-FXB 4.16.10M • 4.16.10FX-7060X 4.16.11M	• 4.15.1FX-7060X.1 • 4.15.1FX-7260QX 4.15.2F 4.15.2.1F 4.15.3F • 4.15.3FX-7050X-72Q • 4.15.3FX-7060X.1 • 4.15.3FX-7060X.2 • 4.15.3FX-7500E3 • 4.15.3FX-7500E3.3 4.15.4F • 4.15.4FX-7500E3 4.15.4.1F 4.15.4.2F 4.15.5M • 4.15.5FX-7500R • 4.15.5FX-7500R-bgpscale • 4.15.5FX-7500R-bgpscale.1 • 4.15.5FX-7500R-bgpscale.2	

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.

		4.16.12M	4.15.5.1M 4.15.6M 4.15.6.1M 4.15.7M 4.15.8M 4.15.9M 4.15.10M	

Affected platforms: All Arista DCS platforms

Resolution: Bug 216203 tracks this vulnerability. EOS-4.19.0F and later releases will contain the fix for this vulnerability. These releases are available on the software downloads page. The following table provides the EOS releases that have the fixes integrated. Releases made available after the initial fixed version will also contain the resolution.

Table-2: Currently Available Remediated EOS releases

4.19	4.18	4.17	4.16	4.15
4.19.0F 4.19.1F		4.17.8M	4.16.13M	

Patch file download URL: SecurityAdvisory0030-Hotfix-v1.1.swix

File URL: SecurityAdvisory0030-Hotfix-v1.1.swix

MD5SUM: 3d29c6d75916a89508eb13bcf537b148

SHA512SUM: 90329906ff83272bb90907d14c7a72b107e3971b15b6263244ee8d49757277505d637ee794b4a98a6b73d6b85b653a4ee36182690b00ee29b07adf91182e76bd

Note:

- The patch is applicable only to EOS versions starting at 4.13.0 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:

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. 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/SecurityAdvisory0030-Hotfix-
v1.1.swix extension:
switch#verify /sha512 flash:SecurityAdvisory0030-Hotfix-v1.1.swix
verify /sha512 (flash:securityAdvisory0030-Hotfix-v1.1.swix) = 90
329906ff83272bb90907d14c7a72b107e3971b15b6263244ee8d49757277505d6
37ee794b4a98a6b73d6b85b653a4ee36182690b00ee29b07adf91182e76bd
```

   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:SecurityAdvisory0030-Hotfix-
v1.1.swix supervisor-peer:/mnt/flash
switch(s2-standby)#copy flash:SecurityAdvisory0030-Hotfix-
v1.1.swix extension:
```

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

```
switch#extension SecurityAdvisory0030-Hotfix-v1.1.swix
```

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

```
switch(s1)#extension SecurityAdvisory0030-Hotfix-v1.1.swix
switch(s2-standby)#extension SecurityAdvisory0030-Hotfix-
v1.1.swix
```

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

```
 switch#show extension
Name                                       Version/Release
    Status extension
------------------------------------------ ----------------------
--- ------ ----
SecurityAdvisory0030-Hotfix-
v1.1.swix      2.77/6375386.erahndnsmasq A, I      1
A: available | NA: not available | I: installed | NI: not install
ed | F: forced
```

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.

```
switch#show version detail | grep SecurityAdvisory0030
dnsmasq-SecurityAdvisory0030 2.77            6375386.erahndnsmasq
UpstreamFixesHotfix0.5
dnsmasq-SecurityAdvisory0030 2.77            5968836.erahndnsmasq
UpstreamFixesHotfix0.59
```

4. Verify that the following message is displayed in /var/log/messages

```
Sep  29 19:22:55
SecurityAdvisory0030: Patch installed successfully
Sep  29 19:22:55
  python: %EXTENSION-6-INSTALLED
: Extension SecurityAdvisory0030-Hotfix-
v1.1.swix  has been installed.
```

5. 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
SecurityAdvisory0030-Hotfix-v1.1.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
```

Note:
This patch (SecurityAdvisory0030-Hotfix-v1.1.swix) will automatically restart the dnsmasq service.
With hotfix v1.0 (SecurityAdvisory0030-Hotfix.swix) that was released with the initial version of this security advisory, it is required to manually restart the dnsmasq service for switches running EOS versions 4.17.0 or later. If the switch was restarted after installing the hotfix v1.0, the switch is already protected and there is no need to restart the dnsmasq.
To manually restart the dnsmasq service the following bash commands can be used.

```
switch#bash
 Arista Networks EOS shell
 [admin@switch ~]$ ps aux | grep dnsmasq
```

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.

```
root 3923 0.0 0.0 4424 1832 ? S Oct06 0:01 /usr/sbin/dnsmasq
arastra 15669 0.0 0.0 4760 1516 pts/5 S+ 12:48 0:00 grep --color=auto
dnsmasq
[admin@switch ~]$ sudo killall dnsmasq
[admin@switch ~]$ sudo service dnsmasq start
Starting dnsmasq: [OK]
[admin@switch ~]$ ps aux | grep dnsmasq
root 16770 0.0 0.0 4424 1832 ? S Oct06 0:01 /usr/sbin/dnsmasq
arastra 16793 0.0 0.0 4760 1516 pts/5 S+ 12:48 0:00 grep --color=auto
dnsmasq
```

The “ps aux | grep dnsmasq” commands are not required to restart dnsmasq, but are used to verify the restart by checking that dnsmasq has a new PID.

Instructions to uninstall the patch:

1. Uninstall the patch using the following command:

```
switch#no extension securityAdvisory0030-Hotfix-v1.1.swix
```

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

```
switch(s1)#no extension securityAdvisory0030-Hotfix-v1.1.swix
switch(s2-standby)#no extension securityAdvisory0030-Hotfix-
v1.1.swix
```

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

```
switch#show extension
Name                                    Version/Release            St
atus extension
---------------------------------------- -------                    --
---- ---------
SecurityAdvisory0030-Hotfix-
v1.1.swix      2.77/6375386.erahndnsmasq  A, NI     1

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

Verify that the following message is displayed in /var/log/messages after uninstalling the

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.

extension

```
Sep  29 20:1
2:47  python: %EXTENSION
-6-UNINSTALLING:
Uninstalling extension securityAdvisory0030-Hotfix-v1.1.swix
....
Sep  29 20:12:47
SecurityAdvisory0030: Patch removed successfully
```

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 to 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

References:

- https://security.googleblog.com/2017/10/behind-masq-yet-more-dns-and-dhcp.html

For more information visit:

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:

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.

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.