Date: April 16th, 2019

Last Updated: April 29th, 2019

Version: 1.1

Revision	Date	Changes
1.0	April 16th, 2019	Initial Release
1.1	April 29th, 2019	Updated with CVE reference and mitigation for impacted versions

The CVE-ID tracking this issue is CVE-2013-7470

CVSSv3 Base Score: 5.9/10 (AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)

Description:

A kernel crash can be triggered remotely through the network by certain malformed packets, specifically by sending an IP packet with rarely used packet options to a switch via a routed port.

This is a publicly found vulnerability and the exposure is specific to EosKernel-3.4 that was used in the EOS releases noted below. Arista is using an updated Kernel version in all of its recent EOS releases and, as such, those versions are not susceptible to this crash or soft lockup.

The Arista EOS versions that are affected, along with the resolution steps, are documented in the following sections.

Vulnerability Assessment for EOS/vEOS:

Affected EOS/vEOS versions

The code releases with Linux kernel version 3.4 are susceptible to this vulnerability. Affected releases are listed below. The release trains starting EOS-4.20 run version 3.18 of the Linux kernel and are not vulnerable.

Affected Software Releases:

4.18	4.19
4.18.10M	4.19.12M

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.

4.18.9M	4.19.11M
4.18.8M	4.19.10M
4.18.7M	4.19.9M
4.18.6M	4.19.8M
4.18.5F	4.19.7M
4.18.4.2F	4.19.6.3M
4.18.4.1F	4.19.6.2M
4.18.4F	4.19.6.1M
4.18.3.1F	4.19.6M
4.18.3M	4.19.5M
4.18.2.1F	4.19.4.1M
4.18.2F	4.19.4M
4.18.1.1F	4.19.3F
4.18.2F	4.19.2.3F
4.18.0F	4.19.2.2F
	4.19.2.1F
	4.19.2F
	4.19.1F
	4.19.0F

Note: EOS release trains from 4.14 to 4.17, that are currently End-of-Software-Support per Arista's software lifecycle policy, also use the impacted kernel version and are susceptible to this vulnerability. Please review the 'Mitigation' and 'Resolution' sections below to evaluate a feasible option for remediation.

Affected Platforms:

This vulnerability is in the Linux kernel and hence affects all platforms running the affected

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.

EOS/vEOS releases.

Symptoms:

The symptom of this exploit would be that of a kernel panic. As a result of this, the system can lead to an unexpected device restart. The kernel crash will point to a soft lockup in cipso_v4_validate. This can be triggered only with certain malformed packets on a routed port.

Resolution:

Bug 155692 tracks this vulnerability. The fix requires an update to the kernel and hence the recommended course of action is to upgrade to a fixed version of EOS.

The fix is available in the following EOS versions in each affected code train:

- EOS-4.18.11M
- EOS-4.19.12.1M

Please upgrade to any of these remediated versions at your earliest convenience.

Mitigation

The long-term resolution is upgrade to a remediated version of EOS. A temporary mitigation is to use a hotfix which can be installed as an EOS extension on any of the affected versions.

It is recommended to install this patch on affected versions of EOS to safeguard against this vulnerability.

Patch file download URL: SecurityAdvisory0040Hotfix.swix

sha512 checksum for verification: 7eea494a74245a06369ed11798bbcd13f6782932ee5586fb289ec6fc5dae4a300bc745a0aec4fb0e348d85d03c2aca37ad97c55313ced0f4c1632888944d2b1d

Note:

- The patch installation is platform independent and hitless. A reload of the switch or any process is not required for the patch to take effect.
- This patch adds iptables rules to do the following actions:
    - Drop any packet with two or more IP options
    - Drop any packet with CIPSO (IP option 134) as its only option.
- This mitigation could potentially have the side effect of dropping traffic that uses multiple IP options or IP option 134. If either of these cases apply, an upgrade is the best solution to address the vulnerability.

For instructions on installation and verification of EOS extensions, refer to this section in the EOS User Manual:
https://www.arista.com/en/um-eos/eos-section-6-7-managing-eos-extensions

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.

References

CVE-2013-7470

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.