Date: May 15th, 2017

Version: 1.0

Revision	Date	Changes
1.0	May 15th, 2017	Initial release

Affected Platforms: All EOS platforms

Affected Software Version: All EOS releases prior to 4.18.1F. The list of affected releases is documented in Table-2.

The CVE-ID tracking this issue is CVE-2017-8231

CVSS v2: 3.5 (AV:N/AC:M/Au:S/C:N/I:N/A:P)

CVSS v3: 4.3 (AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L)

Impact: This advisory is to document a security vulnerability that affects Arista products. The switch's Rib agent can restart when processing an MPBGP update containing a malformed value for a certain specific attribute. Such MPBGP updates are not expected to be received in typical production environments and have to be crafted and sent with the malformed values by a malicious BGP speaker.

Bug188148 and Bug190872 tracks the two potential crashes that can be caused by this vulnerability.

Mitigation:

It is recommended to configure static BGP neighbors with strong BGP authentication keys to protect against unauthorized BGP peers in sending malformed BGP packets.

Bug188148 and Bug190872 are fixed in SW version 4.18.1.

NOTE: This vulnerability was identified internally by Arista Networks and Arista has not received evidence of this being exploited, as of the date of this update.

AFFECTED EOS RELEASES:

Table-2: Affected EOS releases

4.18	4.17	4.16	4.15	Older release trains
4.18.0F	4.17.0F	4.16.6M	4.15.0F	All releases in

	• 4.17.1F • 4.17.1FX-VRRP6LL 4.17.1.1F • 4.17.1.1FX-MDP 4.17.2F • 4.17.2FX-OpenStack 4.17.13F • 4.17.3FX-7500R • 4.17.3FX-7500R.1 4.17.4M 4.17.5M	• 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-7500R • 4.16.7FX-7500R-bgpscale • 4.16.7FX-7060X • 4.16.7FX-7060X.1 • 4.16.7M-L2EVPN • 4.16.7FX-MLAGISSU-TWO-STEP • 4.16.7FX-ECMP-FIX 4.16.8M • 4.16.8FX-7500R • 4.16.8FX-7060X • 4.16.8FX-MLAGISSU-TWO-	• 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-7260QX 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-7500R • 4.15.5FX-7500R-bgpscale 4.15.6M 4.15.7M	4.14 All releases in 4.13 All releases in 4.12 All releases in 4.11 All releases in 4.10 All releases in 4.9 All releases in 4.8 All releases in 4.7 All releases in 4.6 All releases in 4.5 All release trains older than 4.5

		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	4.15.8M 4.15.9M 4.15.10M 4.15.11M	

References:
CVE-2017-8231

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