Date: June 28th, 2016

Version: 1.1

Revision	Date	Changes
1.0	June 15th, 2016	Initial release
1.1	June 28th, 2016	Updated to remove a part of the mitigation section that involved ipv6 ACLs with hop-limit. This section was removed in order to avoid an issue that was recently identified related to ipv6 ACLs with hop-limits. This issue is tracked under **BUG162038**.

NOTE: If you have added the IPv6 ACLs with the "hop-limit" option from the initial release, please remove the hop-limit rules and replace them with the rules suggested. There is a limitation with the hop-limit option that can result in network issues under certain circumstances.

Affected Software Version: All EOS releases after EOS-4.10.0. For a detailed list, please refer to Table-1 below.

Impact: This advisory is to document a security vulnerability that affects Arista products. This vulnerability allows a malicious user to send a flood of specially crafted IPv6 Neighbor Discovery packets from non link-local sources that can fill up the packet processing queue and may cause dropping of legitimate IPv6 Neighbor Discovery packets leading to a denial of service (DoS) condition on the device.

BUG159604 tracks this vulnerability. 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.

AFFECTED EOS RELEASES:

Table-1: Affected EOS releases

4.16	4.15	4.14	4.13	Older release trains
4.16.6M	4.15.0F	4.14.0F	4.13.1.1F	All releases in

	• 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-7500R • 4.15.5FX-7500R-bgpscale	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 4.14.10M 4.14.10.1M 4.14.11M	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	4.10.1*

	4.15.6M	4.14.12M		
* First EOS release to support IPV6 ACL				

Mitigation:

To mitigate against this vulnerability, an ipv6 ACL can be used to drop the invalid ipv6 ND packets. This ACL can be applied to an ipv6 interface wherever applicable. Platform level support per product family is documented in Table-2 below.

The following ACL can be applied at the edge of the network,

```
switch(config)#ipv6 access-list blockForwardingNeighborDiscovery
        10 permit icmpv6 any fe80::/10 133
        20 permit icmpv6 any ff02::/16 133
        30 permit icmpv6 fe80::/10 any 133
        40 deny icmpv6 any any 133
        50 permit icmpv6 any fe80::/10 134
        60 permit icmpv6 any ff02::/16 134
        70 permit icmpv6 fe80::/10 any 134
        80 deny icmpv6 any any 134
        90 permit icmpv6 any fe80::/10 135
        100 permit icmpv6 any ff02::/16 135
        110 permit icmpv6 fe80::/10 any 135
        120 deny icmpv6 any any 135
        130 permit icmpv6 any fe80::/10 136
        140 permit icmpv6 any ff02::/16 136
        150 permit icmpv6 fe80::/10 any 136
        160 deny icmpv6 any any 136
        170 permit icmpv6 any fe80::/10 137
        180 permit icmpv6 any ff02::/16 137
        190 permit icmpv6 fe80::/10 any 137
        200 deny icmpv6 any any 137
        210 permit ipv6 any any
```

In order to check if the switch is probed by attackers, “show ipv6 access-lists” can be used to monitor how many matches are seen for the deny rules.

Table-2: Platform level support per product family

Platform	Release that supports IPv6 ACL
7150 Series	EOS-4.15.0F and later releases
7500E/7280E Series	EOS-4.12.0 and later releases
7050 Series	EOS-4.10.1 and later releases
7304/7308 Series	EOS-4.13.1 and later releases
7010	EOS-4.14.2 and later releases
7500R/7280R Series	EOS 4.15.5FX-7500R and later releases
7060CX/7260CX/7320X	4.15.1FX-7060X and later releases

IPv6 ACLs are not supported in the 7100 Series and 7048 platforms

References:

For more information visit:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1409

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