Date: January 28th 2015

Revision	Date	Changes
1.0	January 28th 2015	Initial release

Arista 7000 Series Products and Arista EOS are not remotely exploitable by CVE-2015-0235

On Jan 27th, information was released about a security advisory for the glibc function __nss_hostname_digits_dots() which could be called via gethostbyname or other similar functions. This vulnerability could allow for a buffer overflow and code execution in affected applications.

A number of customers have contacted Arista Networks, asking if their Arista products are susceptible to the vulnerability. After examining our code base we have determined that we are not vulnerable to remote attackers attempting to make use of this exploit.

Please note that there are several features that use hostnames that are configurable by the switch administrator and may be vulnerable to this CVE. These features require an exec privilege (configuration) level access to set the hostname. Administrators with exec access are already trusted users.

Arista Networks plan to integrate fixes to glibc for currently supported versions of EOS to remove this issue in future versions.

BugID 110326 addresses this issue.

References:
For additional information about the vulnerability, please visit:
http://www.openwall.com/lists/oss-security/2015/01/27/9
https://rhn.redhat.com/errata/RHSA-2015-0090.html
https://access.redhat.com/security/cve/CVE-2015-0235

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.