Date: 9/12/2012

Affected Software Version: EOS-4.8.0 through EOS-4.8.7, EOS-4.9.0 through EOS-4.9.5, EOS-4.10, EOS-4.10.1

Note: You must have IPv6 addresses configured on your system for this to affect you.

Bug 39915: Null pointer dereference in nf_conntrack_ipv6

Impact: A pair of carefully crafted Ipv6 Fragmentation packets may cause a null pointer dereference in the Linux kernel. This will then lead to a kernel panic and the switch rebooting.

Resolution: This is fixed in EOS-4.10.1-SSO, EOS-4.9.6, and EOS-4.10.2 and later.

Workaround: For customers who would prefer to stay on their current version of EOS, the following can be entered from super-user mode on the bash console: ip6tables -t raw -A PREROUTING -m ipv6header --soft --header 44 -j NOTRACK

There is also an extension available - SecAdvisory0002Patch, that can be used to enter the workaround and have it persist across reboot: . The compressed file contains the extension and instructions to install the same.

References:
https://bugzilla.redhat.com/show_bug.cgi?id=833402
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2744

Copyright 2026 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.