Date: October 21st, 2016

Version: 1.0

Revision	Date	Changes
1.0	October 21st, 2016	Initial release

Arista Products vulnerability report for CVE-2016-5195

On October 21st 2016, information was released about a security advisory for a race condition vulnerability in Linux kernel memory subsystem copy on write mechanism.

Arista Network's software products EOS and Cloud Vision Portal (CVP) are not exploitable by CVE-2016-5195 (Kernel Local Privilege Escalation).

Description:

The Linux kernel since version 2.6.22 contains a race condition in the way the copy on write mechanism is handled by the memory subsystem, which may be leveraged locally to gain root privileges. A local, unprivileged attacker can escalate privileges to root.

This security issue relies on the user being able to run a malicious application when logged onto the system. On a standard hardened system that disallows shell access, users are not able to run arbitrary applications, making this a non-issue within Arista products.

References:

https://dirtycow.ninja/

https://access.redhat.com/security/cve/CVE-2016-5195

https://www.kb.cert.org/vuls/id/243144

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 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.