Date: January 3rd, 2018

Version: 1.0

Revision	Date	Changes
1.0	January 3rd, 2018	Initial Release
1.1	January 8th, 2018	Updated description with expanded analysis

Arista Products vulnerability report for the following CVEs:

Spectre
CVE-2017-5753: Bounds check bypass
CVE-2017-5715: Branch target injection

Meltdown
CVE-2017-5754: Rogue data cache load

Arista Networks hardware and software products, including CVP and EOS are not exploitable by the above mentioned CVEs, with an assumption that Arista's recommended security policies are in place.

Description:

On January 3rd 2018, Google's Project Zero released a security advisory for processor based vulnerabilities on Intel corporation and AMD Inc. processors, that could allow local users to read the memory of any process on the system, regardless of the privilege of the user or any separation, such as would be found in a VM environment.

Arista Networks 7000 Series Product Line uses a variety of Intel and AMD CPUs and is hence potentially susceptible to these types of attacks.

However, exploiting this vulnerability requires the ability to run custom code on Arista switches. With the EOS security model, to run custom code a user needs to have root access to the shell. Only trusted users should be given root access. Standard user access restrictions are a suitable mitigation for these CVEs to only allow access from trusted sources and networks. The most foolproof way to prevent exploitation of the CVEs in this advisory is to not allow code from untrusted parties to run on the same CPU. Arista's EOS switches fulfill this requirement.

The following CLI command can be used to check the CPU model:

```
Switch#show management security
```

On Arista vEOS and cEOS products, this vulnerability may be exposed as a result of the underlying hypervisor, kernel and processor behaviors. However any fix or patch to address this issue will only be applicable to the previously mentioned items and not to the Arista product lines.

If CVP is deployed as a VM on hardware shared with untrusted code, there is a potential issue. This should be fixed in the underlying platform. The recommended way to run CVP is via the Arista CloudVision Appliance (CVA) server. This does not run anything other than Arista software and will therefore mitigate the issue.

The Arista engineering team is carefully evaluating the released patches and will consider implementing those patches in future releases, after they have been tested.

References:

CVE-2017-5715 http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5715
CVE-2017-5753 http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5753
CVE-2017-5754 http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5754

Public Information:

https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html

Intel Security Center: https://security-center.intel.com/advisories.aspx

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