Date: October 9th, 2019

Version: 1.0

Revision	Date	Changes
1.0	October 9th, 2019	Initial Release

The CVE-IDs tracking this issue are CVE-2019-14810.

CVSSv3 Base Score: 5.9 (AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)

Description

This advisory is to document a security vulnerability that was identified internally by Arista Networks. Arista has not received evidence of this vulnerability being exploited, as of the date of this update. The vulnerability is in the implementation of the Label Distribution Protocol (LDP) protocol in EOS. Under race conditions, the LDP agent can establish an LDP session with a malicious peer potentially allowing the possibility of a Denial of Service (DoS) attack on route updates and in turn potentially leading to an Out of Memory (OOM) condition that is disruptive to traffic forwarding. Affected EOS versions are listed below. Other Arista software products, such as CloudVision, including on-premises and cloud-based wireless services, Access Points, and 7130 MOS software, are not affected.

Symptoms

Establishing an LDP session with a malicious peer can result in the LDP agent crashing. Repeated attempts could potentially lead to a Denial of Service attack on route updates and potentially an out of memory condition.

Vulnerability Assessment

Affected Software

- EOS
  - 4.22 release train: 4.22.1F and earlier releases
  - 4.21 release train: 4.21.0F - 4.21.2.3F, 4.21.3F - 4.21.7.1M
  - 4.20 release train: 4.20.14M and earlier releases
  - 4.19 release train: 4.19.12M and earlier releases
  - End of support release trains (4.18 and 4.17)

Affected Platforms

Arista platforms that support LDP:

- 7280E/R/R2/R3 series
- 7500E/R/R2/R3 series
- 7020R

Mitigation

An intermediate mitigation is to setup LDP MD5 password configuration on existing sessions. Configure LDP MD5 passwords on both LDP peers:

```
Arista(config)#mpls ldp
Arista(config-mpls-ldp)#password <password-string>
 Arista(config-mpls-ldp)#copy running-config startup-config
```

LDP sessions authenticated with MD5 password are protected from this vulnerability.

Resolution

The vulnerability is tracked by BUG400990 and BUG371998 for EOS. The recommended course of action is to install the provided hotfix or upgrade to a remediated EOS version once available.

Hotfix install instructions:

- The hotfix can be installed as an EOS extension on affected versions (4.17 and later release trains)
- The hotfix restarts the LDP agent and disruption to traffic is limited to just the established LDP sessions. It can take upto 30 seconds for the LDP sessions to re-establish after the installation of the hotfix

Patch file download URL: SecurityAdvisory0042Hotfix.swix
sha512: c94c650c46211cbdfd591865afe7b991b963fa3e153c2d1bb5174febb09160c4fc4bab1b8e08ba437f881a1df79aa00e86c854d5a9fa0e703c0baa15e25fb89c

For instructions on installation and verification of EOS extensions, refer to this section in the EOS User Manual: https://www.arista.com/en/um-eos/eos-section-6-7-managing-eos-extensions. Ensure that the extension is made persistent across reboots by copying the installed-extensions to boot-extensions.

The vulnerability is fixed in the following EOS versions:

- 4.23 release train: 4.23.0F and later releases

- 4.22 release train: 4.22.0.2F and later releases
- 4.22 release train: 4.21.2.4F and the next maintenance release after 4.21.7.1M and later releases
- 4.20 release train: Next maintenance release after 4.20.14M and later releases

Vulnerability References

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14810

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