Date: May 13, 2020

Version: 1.0

Revision	Date	Changes
1.0	May 13, 2020	Initial Release

The CVE-ID tracking this issue: CVE-2020-10188
CVSSv3 Base Score: 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Description:

This security advisory documents the exposure of Arista's products to a security vulnerability in EOS, for customers who use Telnet in their management plane. The vulnerability is in the telnet server (telnetd) and can lead to arbitrary remote code execution by an attacker without requiring credentials.

This is not an Arista specific vulnerability. The exposure in EOS is limited to systems with the telnetd service explicitly enabled (i.e. "management telnet" enabled).

Symptoms

An attack due to this vulnerability could result in remote code execution by an unauthenticated remote attacker. There might not be any logging of the exploitation. The exposure is limited to systems with Telnet enabled.

Vulnerability Assessment

Affected Software

- EOS
  - 4.24.0F
  - 4.23.3M and below releases in the 4.23.x train
  - 4.22.4M and below releases in the 4.22.x train
  - 4.21.10M and below releases in the 4.21.x train
  - All releases in older code trains

Affected Platforms

- This is a platform-independent vulnerability and affects all systems running EOS with the versions identified above
- The following products are **not affected**:
  - Arista Wireless Access Points
  - CloudVision and the CV Servers

- Arista 7130 Systems running MOS
- Big Switch Nodes for BCF and BMF (Arista CCF and DMF)

Mitigation

As a security best practice, it is recommended to use secure alternatives instead of Telnet, which is an unencrypted protocol. EOS offers both SSH and eAPI with TLS as secure management plane protocols. If currently enabled, a prompt mitigation step to safeguard against this vulnerability is to disable Telnet on your Arista systems.

As a resolution against this vulnerability, refer to the section entitled “Resolution” for remediated software versions and hotfix details.

Resolution

This vulnerability is tracked by Bug 472113. If you need to use Telnet in your setup, the recommended course of action is to install the provided hotfix or upgrade to a remediated EOS version.

The vulnerability is fixed in the following EOS versions:

- 4.24.1F and later releases
- 4.23.4M and later releases
- 4.22.5M and later releases
- 4.21.11M and later releases
- 4.24.0.FX-KC

If you are unable to upgrade EOS right away, the fix is available as a hotfix and should be applied to safeguard against this vulnerability.

The hotfix can be installed as an EOS extension and is supported on all affected EOS versions under support. The current oldest supported version of EOS is 4.19.7M. The hotfix installation resets the existing telnet connections. It is non-impactful to traffic forwarding and normal switch behavior.

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.

- Patch file download URL: SecurityAdvisory0048Hotfix.swix
- Sha512sum: ea666cbdc3e6bfcb973aad7fec7c5a324b20844ee234b77df0b8445a62c42d625f1b5dc4228c1eaaa9eb82293f2f1ee76dff67ccc53d3e33db8ae3ca76e24a3a

External References

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10188

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