Date: April 14th, 2020

Version: 1.0

Revision	Date	Changes
1.0	April 14th, 2020	Initial Release

The CVE-ID tracking this issue: CVE-2019-18948
CVSSv3 Base Score: 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Description

This security advisory documents the exposure of Arista's products to a security vulnerability in EOS, specific to the VxLAN implementation. While the mappings already programmed in hardware will not be affected, specific malformed ARP packets can impact the software forwarding of VxLAN packets. This issue is found in Arista's EOS VxLAN code.

The vulnerability is documented by Arista using the following Bug IDs:

- Bug 364633
  - If VxLAN is configured on an MLAG configured system, the VxlanSwFwd agent can crash when receiving certain malformed packets.
- Bug 420663
  - In VxLAN routing setup, certain exceptional packets can cause the VxlanSwFwd agent to restart.

Symptoms

An attack due to this vulnerability could manifest in the form of a crash of the VxlanSwFwd agent. It's not expected that this would impact other agents or traffic forwarding functions. Software forwarding of VxLAN packets may be affected leading to traffic loss, though existing ARP entries or hardware forwarding will not be impacted.

```
VxlanSwFwd: %AGENT-6-INITIALIZED: Agent 'VxlanSwFwd' initialize
```

Vulnerability Assessment

Affected Software

- EOS

- 4.21.8M and below releases in the 4.21.x train
- 4.22.3M and below releases in the 4.22.x train
- 4.23.1F and below releases in the 4.23.x train
- All releases in 4.15, 4.16, 4.17, 4.18, 4.19, 4.20 code train

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 restrict public access to internal devices to safeguard from potential attacks. As a resolution against this vulnerability, refer to the next section for remediated software versions and hotfix details.

Resolution

This vulnerability is tracked by Bug 364633 and Bug 420663 and manifests in VxLAN setups only. The recommended course of action is to install the provided hotfix or upgrade to a remediated EOS version once available.

The vulnerability is fixed in the following EOS versions:

- 4.21.9M and later releases
- 4.22.4M and later releases
- 4.23.2F and later releases

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 version-specific as noted below. The hotfix restarts the VxlanSwFwd agent. During the restart, any new ARP VxLAN requests and replies will be missed however existing ARP entries are not affected. The disruption will last for 5 seconds or less before normal behavior is restored.

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.

- Release versions: 4.20.1-4.20.4.1
  - Patch file download URL: SecurityAdvisory0047Hotfix-4.20.1-4.20.4.1.swix
  - Sha512sum: c566380c1a8e60571170473d7b97a56acf9f278706ec98da8f671b4a0f80c7b88283562da91986cd325f76e6aa17b9fdad4e39a75e115e84463da9fa41d46b9d
- Release versions: 4.20.5-4.20.15
  - Patch file download URL: SecurityAdvisory0047Hotfix-4.20.5-4.20.15.swix
  - Sha512sum: 8269e73f422b5ca49694b95e6b1639479add11752aabf934f109323593277b79752572f5d7611c0719f7e907469e50745b8088fd481ecfa6cec7489692d1e0e7
- Release versions: 4.21.0-4.21.2.4
  - Patch file download URL: SecurityAdvisory0047Hotfix-4.21.0-4.21.2.4.swix
  - Sha512sum: 4330f186c1732c900d7b3b8c31038bcc369b384e619b777fe09a8b404b67ebf746f52cfb7ba2063d2e3bc69f347c19d30fe5b4f7aaa414911637f81ee4921ade
- Release versions: 4.21.3-4.21.8
  - Patch file download URL: SecurityAdvisory0047Hotfix-4.21.3-4.21.8.swix
  - Sha512sum: 1205b2344ee672f63676a16f44c5385e4d0c0b4eca8a0d897ea4709dc7f8eaef0cfb324ae8c539ad44f2e5667b79970d66956324476ac5b1d4844545543657df
- Release versions: 4.22-4.23
  - Patch file download URL: SecurityAdvisory0047Hotfix-4.22-4.23.swix
  - Sha512sum: 5a40fc6dfceec072cf9d6b68a78158c4f84f1eeb6335afe1c7e9a0eba174c7f4e9f72918b5fd903fae92c47d1ea01b179868c4a8e1d890efe0d704ae56039909

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