Date: September 13th, 2018

Version: 1.0

Revision	Date	Changes
1.0	September 13th, 2018	Initial Release

The CVE-ID tracking this issue is CVE-2018-14008

CVSS v3: 6.5/10 (AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Description

This advisory is to document a security vulnerability that affects EOS. The affected feature is 802.1x authentication, and by extension MACSec when dynamic keys are used. The vulnerability allows for crashing the Dot1x agent via a crafted packet sent from the data port which could result in a denial of service attack at the data plane preventing other users from successfully authenticating with the device. This vulnerability was identified internally by Arista Networks and Arista has not received evidence of this being exploited, as of the date of this update.

Bug ID: 275350

Affected EOS versions:

4.21	4.20	4.19	4.18	4.17	4.16	All older release trains
4.21.0F	4.20.8M 4.20.7M 4.20.6F 4.20.5.2F 4.20.5.1F 4.20.5F 4.20.4.1F 4.20.4F 4.20.3F 4.20.2.1F 4.20.2F 4.20.1F 4.20.0F	4.19.9M 4.19.8M 4.19.7M 4.19.6.3M 4.19.6.2M 4.19.6.1M 4.19.6M 4.19.5M 4.19.4.1M 4.19.4M 4.19.3F 4.19.2.3F 4.19.2.2F 4.19.2.1F 4.19.2F 4.19.1F	4.18.8M 4.18.7M 4.18.6M 4.18.5M 4.18.4.2F 4.18.4.1F 4.18.4F 4.18.3.1F 4.18.3F 4.18.2.1F 4.18.2F 4.18.1.1F 4.18.1F 4.18.0F	4.17.9M 4.17.8M 4.17.7M 4.17.6M 4.17.5.1M 4.17.5M 4.17.4M 4.17.3F 4.17.2.1F 4.17.2F 4.17.1.4F 4.17.1.1F 4.17.1F 4.17.0F	4.16.14M 4.16.13M 4.16.12M 4.16.11M 4.16.10M 4.16.9M 4.16.8M 4.16.7M 4.16.6M	All release trains older than 4.15

		4.19.0F				

Affected Platforms

802.1x is a platform independent feature. All platforms are affected.

Symptoms

The Dot1x agent crash would be a symptom when receiving malicious packets from a supplicant. Relevant observation would be failing for 802.1x authentication, and by extension MACsec. The impact to MACsec would be only when dynamic keys are used ("key source dot1x" should appear in the macsec profile for this vulnerability to affect MACsec).

This vulnerability can be exploited only if the 802.1x feature has been configured.

Mitigation

It is recommended to install this patch on affected versions of EOS to safeguard against this vulnerability.

Patch file download URL: SecurityAdvisory0038Hotfix.swix

sha256sum is: fa9687080df6dd5602f835abf8f34660b66c651711d17310b89eadb5807f5c3f
sha512sum is: 3f764e58f7b090f5ad70d51e080298f753907578f2a41f998a2dab18304fffc6d329
a600dc8b32e3dee1ebf2ad202116f663c6909c2c690581ca393746b4247e

Note:

- The patch installation is hitless and a reload of the switch is not required for the patch to take effect
- This hotfix is EOS dependent and can be patched with the following versions:
    - 4.20.8M
    - 4.20.7M
    - 4.20.4.1F
    - 4.19.9M
    - 4.18.8M

Instructions to install the patch:

1. Download the patch file and copy the file to the extension partition of the switch using one of the supported file transfer protocols:

```
switch#copy scp://10.10.0.1/SecurityAdvisory0038Hotfix.swix exten
sion:
switch#verify /sha512 extension:SecurityAdvisory0038Hotfix.swix
verify /sha512 (extension:SecurityAdvisory0038Hotfix.swix) = 3f76
4e58f7b090f5ad70d51e080298f753907578f2a41f998a2dab18304fffc6d329a
```

```
600dc8b32e3dee1ebf2ad202116f663c6909c2c690581ca393746b4247e
```

2. Verify that the checksum value returned by the above command matches the provided checksum for the file
3. Install the patch using the extension command. The patch takes effect immediately at the time of installation.

```
switch#extension SecurityAdvisory0038Hotfix.swix
```

4. Verify that the patch is installed using the following commands:

```
switch#show extensions
Name                                  Version/Release      Status
     Extension
------------------------------------ -------------------- -------
---- ---------
SecurityAdvisory0038Hotfix.swix      1.0.0/eng            A, I
     1
```

5. Make the patch persistent across reloads. This ensures that the patch is installed as part of the boot-sequence. The patch will not install on EOS versions with the security fix.

```
switch#copy installed-extensions boot-extensions
switch#show boot-extensions
SecurityAdvisory0038Hotfix.swix
```

6. For dual-supervisor systems, ensure the patch is installed on both supervisors by following the steps documented above. Copy the patch to flash of both the supervisors and follow the procedure outlined above.
   For additional guidance on the installation of extensions, refer to the Arista Configuration Guide: https://www.arista.com/en/um-eos

Resolution:

Bug 275350 tracks this vulnerability for EOS. The fix for this issue will be available starting in the following EOS releases:

- 4.21.2.3F
- 4.21.1F
- 4.20.9M (available as of the date of advisory posting)
- 4.19.10M (available as of the date of advisory posting)
- 4.18.10M

Please install the provided hotfix as a mitigation until the remediated versions are available.

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