**Date: October 19th, 2021**

**Version: 1.0**

| Revision | Date | Changes |
|---|---|---|
| 1.0 | October 19th, 2021 | Initial Release |

## Security Advisory 0069

The CVE-ID tracking this issue: CVE-2021-28496
CVSSv3.1 Base Score: 5.7( CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

## Description

This advisory documents the impact of an internally found vulnerability in Arista's EOS software. Affected software releases are listed below.

The effect of this vulnerability is that, when using shared secret profiles the password configured for use by BiDirectional Forwarding Detection (BFD) will be leaked when displaying output over eAPI or other JSON outputs to authenticated users on the device.

This issue was discovered internally and Arista is not aware of any malicious uses of this issue in customer networks.

## Vulnerability Assessment

### Affected Software

EOS Versions

- All releases in 4.22.x train
- 4.23.9 and below releases in the 4.23.x train
- 4.24.7 and below releases in the 4.24.x train
- 4.25.4 and below releases in the 4.25.x train
- 4.26.1 and below releases in the 4.26.x train

### Affected Platforms

This is a platform-independent vulnerability and affects all systems running EOS and CloudEOS with the versions identified above.

The following products are **not** affected:

- Arista Wireless Access Points
- CloudVision WiFi, virtual appliance or physical appliance
- CloudVision WiFi cloud service delivery

- CloudVision Portal, virtual appliance or physical appliance
- CloudVision as-a-Service
- Arista 7130 Systems running MOS
- Arista Converged Cloud Fabric and DANZ Monitoring Fabric (Formerly Big Switch Nodes for BCF and BMF)
- Awake Security Platform

## Mitigation

The following configuration changes may be used as an immediate mitigation in order to prevent the exploitation temporarily. Please upgrade to the fixed version or install the hotfix swix as the proper final resolution, which can be referred to the Resolution section below with details of the remediated software versions.

The restriction of access to the related CLI show command of specified role type can be used as an immediate mitigation. The detailed instructions of role-based authorization can be found here.

Example:

1. Create a new role with restricted access to the CLI show command and make sure the rule has been successfully configured

```
switch(config)#role sysadmin
switch(config-role-
sysadmin)#deny command show management security session shared-secret profile
switch(config-role-sysadmin)# permit command .*
switch(config-role-sysadmin)#exit

switch#show users roles sysadmin
The default role is network-operator

role: sysadmin
        10 deny command show management security session shared-secret profile
        20 permit command .*
```

   Note: in the example above, all other commands besides the show shared profile CLI commands are permitted, it can be tightened up further to only allow commands needed for role sysadmin.
2. Enable role-based access control

```
switch(config)#aaa authorization commands all default local
```

3. Assign the role to a username

Roles are assigned to local users through the username command and to remote users through RADIUS servers. Each user is assigned one role. Each role can be assigned to multiple local and remote users.

```
switch(config)#username adminUser privilege 15 role sysadmin secret adminUserPassword
```

4. Login with username “adminUser” should deny the access of shared-secret profile CLI show command

```
switch#show management security session shared-secret profile
% Authorization denied for command 'show management security session shared-secret profile'
```

## Resolution

This vulnerability is being tracked by BUG607643. The recommended resolution is to upgrade to a remediated software version at your earliest convenience.

The vulnerability is fixed in the following EOS versions:

- 4.23.10 and later releases
- 4.24.8 and later releases
- 4.25.5 and later releases
- 4.26.2 and later releases

For an immediate remediation until EOS can be upgraded, the following hotfixes are available.

The hotfix can be installed as an EOS extension and is version-specific as noted below. Please note the hotfix restarts the ConfigAgent, which will result in all CLI sessions on ssh and console to be logged out and new CLI sessions to not be possible until the ConfigAgent has fully restarted. The disruption will last for 1 minutes or less before normal behavior is restored. It might in rare situations also cause BFD sessions to flap briefly.

- Release versions: 4.22.0 - 4.25.0
    - URL: SecurityAdvisory0069Hotfix-4.22-4.25.0.swix
    - SWIX hash: (SHA512)36fc77d7ff5de2aacfff822bac4e054137a5ebf7d54f283cd4d4be05f15a2c1e448245080e0be11122831bb672d1d777724a8bcbbf029e32a3611d6002e2cf10
- Release versions: 4.25.1 - 4.26.1

- URL: SecurityAdvisory0069Hotfix-4.25.1-4.26.1.swix
- SWIX hash: (SHA512)c8d5a8ab801c7e45dbc0f062f738f3af72084b451a7734c5607a884d648d88b37d7a8451d09dd0a051728199f4b6b0c0bef76b5c3862a668298410cbce55e085

For instructions on installation and verification of the hotfix patch, refer to the "managing EOS extensions" section in the EOS User Manual. Ensure that the patch is made persistent across reboots by running the command '***copy installed-extensions boot-extensions***'.

## 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