Date: November 10, 2026

Revision	Date	Changes
1.0	November 10, 2026	Initial release

The CVE-ID tracking this issue: CVE-2026-102166
CVSSv3.1 Base Score: 8.8 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CVSSv4.0 Base Score: 9.4
(CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H)
CWE: CWE-798: Use of Hard-coded Credentials
This vulnerability is being tracked by BUG 1846906

Description

Arista C-260 and C-250 access points ship with fleet-wide static cryptographic keys used for firmware image verification and SSLP authentication. An attacker who is able to access these keys would be able to create modified firmware that will pass verification checks. This vulnerability is specific to the C-260 and C-250 models; other access point models enforce digitally signed upgrade images with secure boot and are not affected by this issue.

This issue was discovered internally by Arista, and the company is not aware of any malicious exploitation of this vulnerability in customer networks.

Vulnerability Assessment

Platform and Software Applicability Note

To determine actual exposure, operators should first check their software versions against the "Affected Software" list below. If your software release is not listed, your deployment is not vulnerable, regardless of the hardware platform in use.

Affected Software

Wi-Fi Access Point

- All AP releases

Affected Platforms

The following products **are** affected by these vulnerabilities:

- Wi-Fi Access Points C-260
- Wi-Fi Access Points C-250

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

The following products **are not** affected by these vulnerabilities:

- Arista EOS-based products:
  - 710 Series
  - 720D Series
  - 720XP/722XPM Series
  - 750X Series
  - 7010TX Series
  - 7020R/R4 Series
  - 7130 Series running EOS
  - 7170 Series
  - 7050X3/X4 Series
  - 7060X/X2/X4/X5/X6/XE7 Series
  - 7260X/X3 Series
  - 7280R/R2/R3/R4 Series
  - 7300X/X3 Series
  - 7320X Series
  - 7358X4 Series
  - 7368X4 Series
  - 7388X5 Series
  - 7500R/R2/R3 Series
  - 7800R3/R4 Series
  - 7700R4 Series
  - AWE 5000 Series
  - AWE 7200R Series
  - ZTX-7200 Series
  - CloudEOS
  - cEOS-lab
  - vEOS-lab
  - CloudVision eXchange, virtual or physical appliance
- CloudVision Portal on-premises, virtual appliance or physical appliance (including the CV-CUE on premises software)
- CloudVision CUE cloud service delivery
- CloudVision Appliance Software
- CloudVision as-a-Service
- CloudVision AGNI - Cloud service delivery
- CloudVision AGNI - Virtual or physical appliance
- Arista Converged Cloud Fabric (formerly Big Switch BCF)
- DANZ Monitoring Fabric (DMF) - Controller Appliance
- DANZ Monitoring Fabric (DMF) - Analytics Node Appliance
- DANZ Monitoring Fabric (DMF) - Recorder Node Appliance
- DANZ Monitoring Fabric (DMF) - Service Node Appliance
- Arista Multi Cloud Director (formerly Big Switch MCD)
- Arista Network Detection and Response (NDR) Security Platform (Formerly Awake NDR)
- Arista Edge Threat Management - Arista NG Firewall and Arista Micro Edge (Formerly

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

Untangle)
- Arista NetVisor OS, Arista NetVisor UNUM, and Insight Analytics (Formerly Pluribus)
- VeloCloud Orchestrator (Formerly VeloCloud Orchestrator by Broadcom)
- VeloCloud Gateway (Formerly VeloCloud Gateway by Broadcom)
- VeloCloud Edge (Formerly VeloCloud Edge by Broadcom)

Required Configuration for Exploitation

This vulnerability is specific to the C-260 and C-250 access point models. No specific configuration is required. Other access point models enforce digitally signed firmware upgrades and are not affected.

Indicators of Compromise

No indicators of compromise are available for this issue.

Mitigation

To ensure all firmware upgrades undergo mandatory digital signature verification, customers are advised to disable the HMAC-based firmware verification fallback path on affected access points.

Cloud Management

Please contact the Arista TAC for assistance in disabling this path.

On-Prem Deployment

For On-prem deployments, first identify the active HA node. Apply the change only on the active node.

1. On the active node, enter the Wi-Fi Manager container using nerdctl exec with root access from CVP shell.

```
nerdctl exec -it wifimanager -- bash
```

2. From inside the container, run the config CLI command set config parameter and update the upgrade_hmac_fallback_enabled parameter to 0 for configid 1 and 3.
3. Restart sserverd after updating the parameter so the change takes effect.

```
[root@cvml-10-243-248-71 ~]# nerdctl exec -it wifimanager -- bash
[root@wifi-security-server1 /]# su - config
[Last login: Tue Nov  3 15:46:35 UTC 2026 from 10.95.66.215 on pts/3
```

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

```
Welcome to the Server Config Shell.
Type "help" to list available commands in this shell.

Note: Bash style tabbed command completion, command
history and command line editing are supported by this
shell. This shell works best when used in full screen
mode

To configure backspace, use the 'set erase' command.
[config]$ set config parameter
Sets a configuration parameter directly in the database. You must know the exa
ct name, ID and value of the database parameter to use this command.
 >
Enter parameter name: upgrade_hmac_fallback_enabled
Enter parameter value: 0
Enter configid: 3

Current value of parameter [upgrade_hmac_fallback_enabled] is [0]

Do you want to update [upgrade_hmac_fallback_enabled] to [0] in configid [3]?
(y/n):y
[Value of parameter [upgrade_hmac_fallback_enabled] has been updated successfu
lly.
Skipping Aeris sync for configuration parameter [upgrade_hmac_fallback_enabled
] because [FT_TOGGLE_CONFIG_PARAMS_TO_AERIS] is disabled for instance Id: [0].
[config]$ set config parameter
Sets a configuration parameter directly in the database. You must know the exa
ct name, ID and value of the database parameter to use this command.

Enter parameter name: upgrade_hmac_fallback_enabled
Enter parameter value: 0
Enter configid: 1

Current value of parameter [upgrade_hmac_fallback_enabled] is [0]

Do you want to update [upgrade_hmac_fallback_enabled] to [0] in configid [1]?
(y/n):y
[Value of parameter [upgrade_hmac_fallback_enabled] has been updated successfu
lly.
Skipping Aeris sync for configuration parameter [upgrade_hmac_fallback_enabled
] because [FT_TOGGLE_CONFIG_PARAMS_TO_AERIS] is disabled for instance Id: [0].
[config]$ exit
[Exits the config shell session.
```

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

```
[root@wifi-security-server1 /]# /etc/init.d/sserverd restart
Stopping sserverd:                                 [  OK  ]

Starting sserverd:                                 [  OK  ]
[root@wifi-security-server1 /]#
```

Resolution

No fixed release version available for this issue.

Hotfix

No hotfix is available for this issue.

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: List of regional telephone numbers

Receive notification for new advisories and notices:

Subscribe to the RSS feed and email notifications to receive periodic updates on new software releases, advisories, end of sale and field notices.

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.