Date: October 6, 2026

Revision	Date	Changes
1.0	October 6, 2026	Initial release
1.1	October 13, 2026	Updated Resolution section to include the 2026.3.0 release

Description

All CVEs covered in this advisory affect platforms running CloudVision Portal (on-premises) where OpenID Connect (OIDC)-based single sign-on (SSO) is configured with an identity provider. OIDC SSO is an optional, explicitly configured authentication method. Deployments using non-OIDC SSO methods are not affected.

The below issues were discovered internally by Arista, and the company is not aware of any malicious exploitation of these vulnerabilities in customer deployments.

CVE-2026-101149

Insufficient validation of OIDC SSO provider configuration could allow a user with specific high privileges to direct requests to arbitrary destinations.
CVSSv3.1 Base Score: 4.1 (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N)
CVSSv4.0 Base Score: 5.1
(CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:N/VI:N/VA:N/SC:L/SI:N/SA:N)
Common Weakness Enumeration: CWE-918: Server-Side Request Forgery (SSRF)
This vulnerability is being tracked by BUG 1919444

CVE-2026-101150

Insufficient validation of OIDC bearer token configuration could allow a user with specific high privileges to direct requests to arbitrary destinations.
CVSSv3.1 Base Score: 4.1 (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N)
CVSSv4.0 Base Score: 5.1
(CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:N/VI:N/VA:N/SC:L/SI:N/SA:N)
Common Weakness Enumeration: CWE-918: Server-Side Request Forgery (SSRF)
This vulnerability is being tracked by BUG 1919438

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

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.

vulnerable, regardless of the hardware platform in use.

Affected Software

CloudVision Portal Versions

CVE-2026-101149

The following releases are affected:

- 2026.2.0
- 2026.1.2 and below releases in the 2026.1.x train
- 2025.3.3 and below releases in the 2025.3.x train
- All prior releases back to and including 2020.3.0

CVE-2026-101150

The following releases are affected:

- 2026.2.0
- 2026.1.2 and below releases in the 2026.1.x train
- 2025.3.3 and below releases in the 2025.3.x train
- All prior releases back to and including 2023.3.0

Affected Platforms

The following products **are** affected by this vulnerability:

- CloudVision Portal, virtual appliance or physical appliance (Note: CV-CUE on-premises is not affected)

The following product versions and platforms **are not** affected by this vulnerability:

- 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 Series

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.

    - 7260X/X3 Series
    - 7280R/R2/R3/R4 Series
    - 7300X/X3 Series
    - 7320X Series
    - 7358X4 Series
    - 7368X4 Series
    - 7388X5 Serie
    - 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
- Wi-Fi Access Points
- CloudVision CUE, virtual appliance or physical appliance
- CloudVision CUE cloud service delivery
- CloudVision Appliance Software
- CloudVision as-a-Service
- CloudVision AGNI - Cloud service delivery
- CloudVision AGNI - Virtual or physical appliance
- Arista 7130 Systems running MOS
- 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 DANZ Monitoring Fabric (formerly Big Switch BMF)
- 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 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

Both CVEs require that an OIDC identity provider has been configured.

CVE-2026-101149

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.

In order to be vulnerable to CVE-2026-101149, OAuth SSO must be configured.

To verify, navigate to **Settings ? Access Management ? Authentication ? SSO Providers**. If any provider appears under the **OAuth Providers** section, OAuth SSO is configured. If no provider is listed, there is no exposure to this issue.

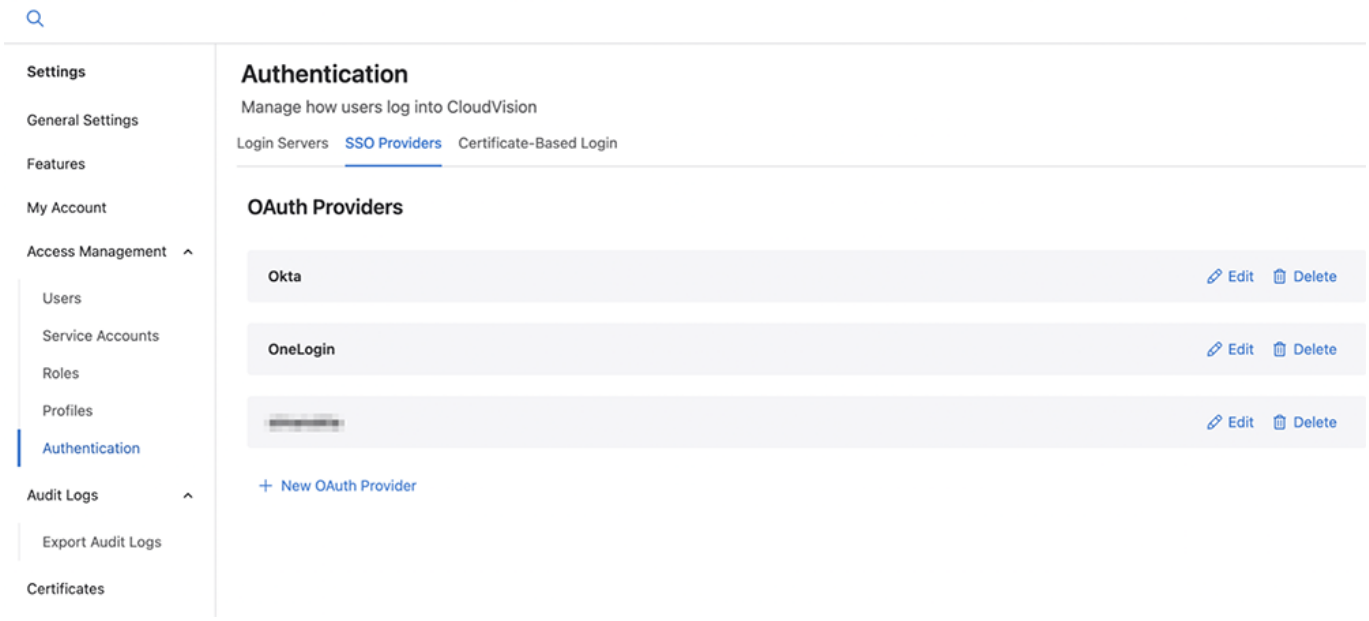


Fig 1: Authentication page showing configured OAuth SSO providers

CVE-2026-101150

In order to be vulnerable to CVE-2026-101150, OAuth SSO must be configured (see Fig 1 above), and **Allow Bearer Token Login** must be enabled in cluster management settings.

To verify, navigate to **General Settings ? Cluster Management**. If the "*Allow Bearer Token Login"* toggle is disabled, there is no exposure to this issue.

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.

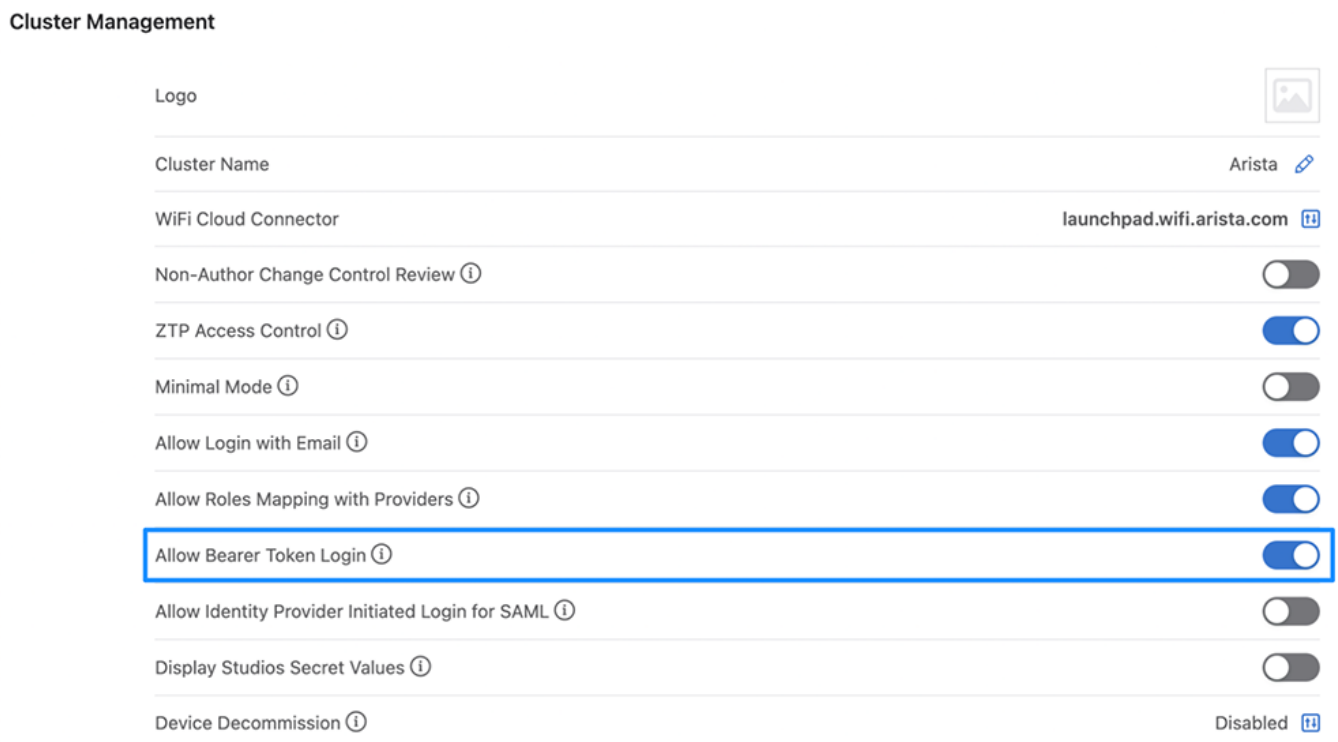


Fig 2: Bearer token login toggle in Cluster Management Settings

Indicators of Compromise

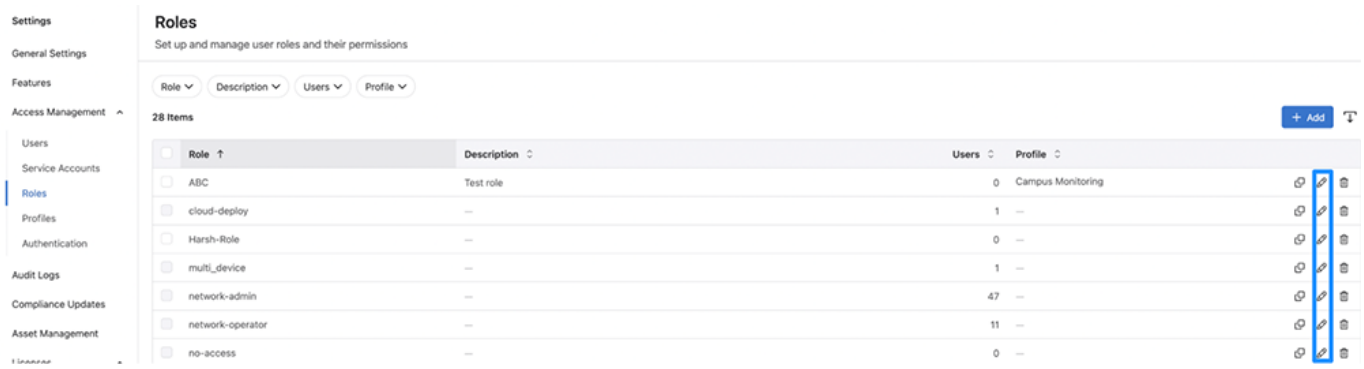
No indicators of compromise exist for both the issues.

Mitigation

There is no configuration-based mitigation for these issues. However, operators can look into switching to an alternative non-OIDC SSO login method, if feasible.

Additionally, restrict AAA settings & Account Management configuration permissions to trusted personnel only.

To do this, navigate to **Settings ? Roles**, then click on the "Pencil" icon beside a role to edit it.



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.

Fig 3: Roles settings page

Ensure that only administrative roles have “**Read and Write**” permission on *AAA Settings* and *Account and Session Management*

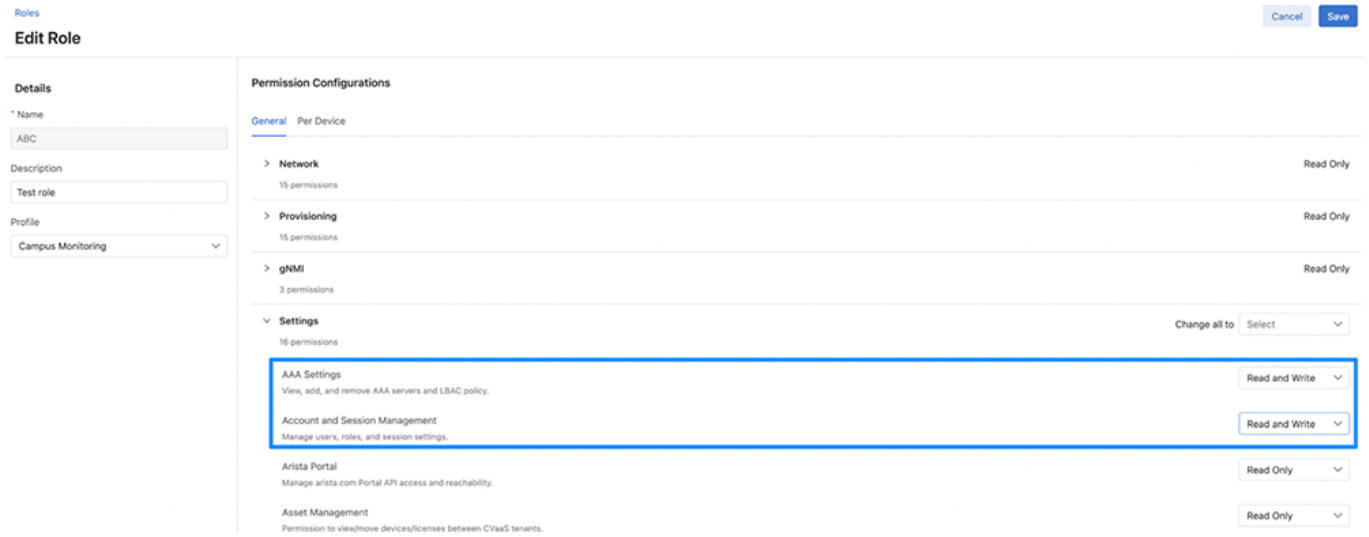


Fig 4: Configuring a Role

Then, go to **Settings ? Users**. Ensure that only trusted personnel have administrative roles.

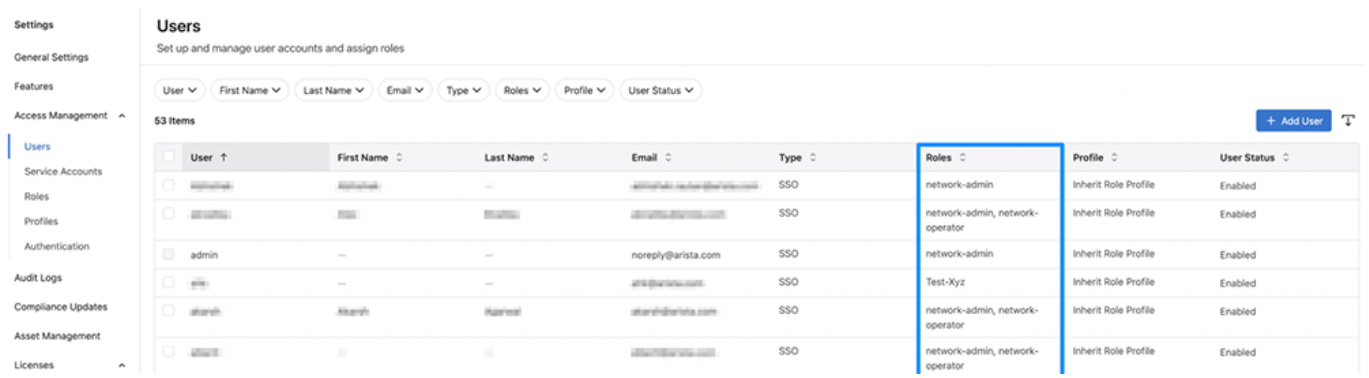


Fig 5: Users settings page

Resolution

The recommended resolution is to upgrade to a remediated software version at your earliest convenience. Arista recommends customers move to the latest version of each release that contains all the fixes listed below. For more information about upgrading see CloudVision Users Manual: Upgrade.

CVE-2026-101149 and CVE-2026-101150 has been fixed in the following releases:

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.

- 2026.3.0 and later releases in the 2026.3.x train
- 2026.2.1 and later releases in the 2026.2.x train
- 2026.1.3 and later releases in the 2026.1.x train
- 2025.3.4 and later releases in the 2025.3.x train

Hotfix

No hotfix is available for these issues.

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

Contact information needed to open a new service request may be found at:
https://www.arista.com/en/support/customer-support

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.