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 CloudVision Portal (On-Premises), where specially crafted requests could result in user redirection to arbitrary URLs.

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-2026-101151

Insufficient validation of request in login flow could allow a remote, unauthenticated attacker to craft a URL that, when clicked by a user, redirects the user's browser to an arbitrary external site upon completion of the authentication process.
CVSSv3.1 Base Score: 4.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N)
CVSSv4.0 Base Score: 5.3
(CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-601: URL Redirection to Untrusted Site ('Open Redirect')
This vulnerability is being tracked by BUG 1612748

CVE-2026-101152

Insufficient validation in the Single Sign-On (SSO) login flow could allow a remote, unauthenticated attacker to craft a URL that, when clicked by a user, causes the identity provider (IdP) to deliver authentication material to an attacker-controlled URL instead of to CloudVision.
CVSSv3.1 Base Score: 8.0 (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:N)
CVSSv4.0 Base Score: 7.6
(CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:P/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N)
Common Weakness Enumeration:CWE-601: URL Redirection to Untrusted Site ('Open Redirect')
This vulnerability is being tracked by BUG 1864515

Vulnerability Assessment

Platform and Software Applicability Note

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.

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

CloudVision Portal Versions

CVE-2026-101151

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-2026-101152

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 2021.1.0

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

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.

    - 7050X3/X4 Series
    - 7060X/X2/X4/X5/X6 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
- 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
- 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 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

CVE-2026-101151

No specific configuration is required to be vulnerable to this issue. This vulnerability is present in

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 default configuration of affected CloudVision releases.

CVE-2026-101152

In order to be vulnerable to CVE-2026-101152, SSO must be configured with an external identity provider. Deployments using only non-SSO authentication are not affected.

To check if SSO is configured, navigate to **Settings ? Authentication** in the CloudVision UI. If an OIDC or SAML provider is configured, the deployment is potentially affected.

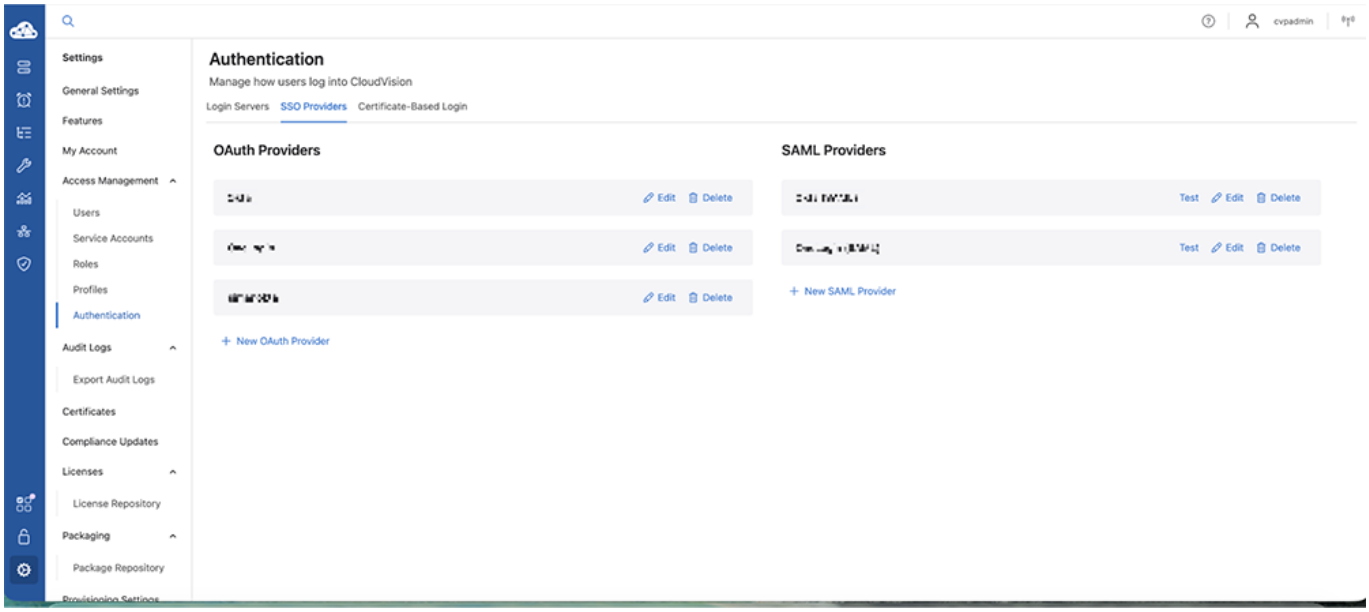


Fig 1: Page showing configured SSO providers

Indicators of Compromise

No indicators of compromise exist for both the issues.

Mitigation

No mitigation exists for both the issues.

Resolution

CloudVision Portal

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.

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.

CVE-2026-101151 and CVE-2026-101152 have been fixed in the following releases:

- 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.