Date: September 9, 2026

Revision	Date	Changes
1.0	September 9, 2026	Initial release
1.1	September 22, 2026	CSAF JSON file added

The CVE-ID tracking this issue: CVE-2026-73439
CVSSv3.1 Base Score: 7.5 (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)
CVSSv4.0 Base Score: 7.7
(CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-842: Placement of User into Incorrect Group
This vulnerability is being tracked by BUG 1602638

Description

On affected platforms running Arista EOS, if OpenConfig is configured and running a gNMI (gRPC Network Management Interface) server on the system, and if gNSI (gRPC Network Security Interface) Pathz is configured and a gNSI Pathz policy is present on the system, then gNMI may fail to correctly enforce the rules in this policy if both a group rule and a user rule for the same path is present in the policy. Under certain conditions, this can lead to an authenticated user gaining unauthorized permission to read or write gNMI paths that the Pathz policy is intended to restrict.

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

Vulnerability Assessment

Affected Software

EOS Versions

- 4.36.0.1F and below releases in the 4.36.x train
- 4.35.5M and below releases in the 4.35.x train
- 4.34.6M and below releases in the 4.34.x train
- From 4.33.2F through 4.33.8M in the 4.33.x train

Affected Platforms

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

- Arista EOS-based products:

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.

- 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
- 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
- CloudEOS
- cEOS-lab
- vEOS-lab
- CloudVision eXchange, virtual or physical appliance

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

- Arista Wireless Access Points
- CloudVision CUE, virtual appliance or physical appliance
- CloudVision CUE cloud service delivery
- CloudVision Portal, virtual appliance or physical appliance
- 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)

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.

- 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

In order to be vulnerable to CVE-2026-73439, all of the following conditions must be met:

- OpenConfig must be configured with a gNMI transport started
- gNSI must be configured with the gNSI Pathz service enabled.
- A pathz policy must be present on the system, with at least one group rule in the policy and at least one user rule in the policy.

If OpenConfig is configured with a gNMI transport, the running configuration will include:

```
management api gmni
  transport grpc <name>
```

Where <name> is the name of the transport.

If gNSI is configured with the gNSI Pathz service enforced, the running configuration will include:

```
management api gnsi
  service pathz
```

The config may also reference a gRPC transport which would be used to run the gNSI Pathz service and perform policy rotation:

```
management api gnsi
  transport gnmi <name>
  service pathz
```

If a Pathz policy (if present on the system) will be at the path **/persist/sys/gnsi/pathz/policy.json**

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 check for the presence of the policy here, run the following commands:

```
switch>enable
switch#bash stat /persist/sys/gnsi/pathz/policy.json
```

The Pathz policy must contain at least one group rule and at least one user rule for the same path, so the **/persist/sys/gnsi/pathz/policy.json** file will contain a rule entry with “group” specified as the principal, and another with “user” specified as the principal, and the same path used in both instances.

For example the following rule uses the group “some-group” as the principal, and /system as the path:

```
{
  "id": "abc",
  "group": "some-group",
  "path": ]},
  "action": "ACTION_PERMIT",
  "mode": "MODE_READ"
}
```

And the following rule uses the user “bob” as the principal and /system as the path:

```
{
  "id": "def",
  "user": "bob",
  "path": ]},
  "action": "ACTION_PERMIT",
  "mode": "MODE_READ"
}
```

Indicators of Compromise

An indicator of compromise would be if a gNMI Client is able to access any YANG paths which should be inaccessible given the rules specified in the current pathz policy.

Mitigation

One possible mitigation to this is to disable gNSI Pathz.
This can be done with the following configuration:

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.

```
switch#configure
switch(config)#management api gnsi
switch(config-mgmt-api-gnsi)#no service pathz
```

Another possible mitigation is to push a new gNSI Pathz policy to the system (using the gNSI Pathz Rotate RPC), where this policy does not contain any group rules.

To push a new policy, initiate a Pathz Rotate RPC with your client. Using grpcurl, to an insecure server for a user with no password, this would look like:

```
grpcurl -protoset ./pathz.proto.pb -H 'username:$USER' -v -d @ -plaintext $TARGET:$PO
RT gnsi.pathz.v1.Pathz/Rotate  << EOF
{
 "upload_request" : {
     "version": <version>,
     "created_on":<timestamp>,
     "policy": <policy>
 }
}
{
 "finalize_rotation":
}
EOF
```

For example, to push a policy allowing the users “alice” and “bob” access to **/system**, push a policy like so:

```
grpcurl -protoset ./pathz.proto.pb -H 'username:$USER' -v -d @ -plaintext $TARGET:$PO
RT gnsi.pathz.v1.Pathz/Rotate  << EOF
{
 "upload_request" : {
  "version": "v0",
  "created_on": 1675786127456593000,
  "policy":
     {"rules":[{
         "id":"abc",
         "user":"alice",
         "path":]},
        "action":"ACTION_PERMIT",
        "mode":"MODE_READ"
      },{
```

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.

```
          "id":"xyz",
          "user":"bob",
          "path":]},
         "action":"ACTION_PERMIT",
         "mode":"MODE_READ"
       }]
     }
  }
}
{
 "finalize_rotation":
}
EOF
```

Note the rules are using the “user” principal, so as to avoid being subject to this CVE, and that rules are duplicated for each user, rather than putting these in a group.

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 EOS User Manual: Upgrades and Downgrades

CVE-2026-73439 has been fixed in the following releases:

- 4.36.1F and later releases in the 4.36.x train
- 4.35.6M and later releases in the 4.35.x train
- 4.34.7M and later releases in the 4.34.x train
- 4.33.9M and later releases in the 4.33.x train

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

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.

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.