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-2026-73453
CVSSv3.1 Base Score: 10.0 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
CVSSv4.0 Base Score: 9.5
(CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H)
Common Weakness Enumeration: CWE-94: Improper Control of Generation of Code ('Code Injection')
This vulnerability is being tracked by BUG 1850014

Description

An unauthenticated P4Runtime (Programming Protocol-Independent Packet Processors Runtime) client can achieve arbitrary code execution under certain conditions on affected platforms running Arista EOS configured with P4Runtime. **P4Runtime is disabled by default in Arista EOS.** By crafting a malicious packet during the initiation of a P4Runtime session, an attacker can obtain complete administrative control over the compromised switch.

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

EOS Versions

- 4.36.1F and earlier releases in the 4.36.x train
- 4.35.5M and earlier releases in the 4.35.x train
- 4.34.7M and earlier releases in the 4.34.x train
- All releases in the 4.33.x train
- All releases in the 4.32.x train
- All releases in the 4.31.x train

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.

- All releases in the 4.30.x train
- All releases starting from 4.29.2F in 4.29.x train

Affected Platforms

The following products **are** 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
  - 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
  - CloudEOS
  - cEOS-lab
  - vEOS-lab
  - CloudVision eXchange, virtual or physical appliance

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

- Wi-Fi 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

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 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 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

In order to be vulnerable to CVE-2026-73453, the following condition must be met:

p4-runTime must be configured in one of the following combinations. P4-runtime is not a feature which runs by default and must be explicitly enabled:

1. Non TLS mode (p4-runtime is enabled with no ssl profile configured)

```
switch>show p4-runtime
Enabled: yes
Server: running on port 9559, in mgmtVrf VRF
SSL profile: none
Authentication username priority: x509-spiffe, x509-common-name
Total clients: 0
Accounting requests: no
```

2. TLS mode (p4-runtime is enabled and ssl profile is configured with no trusted certificates)

```
switch>show p4-runtime
Enabled: yes
Server: running on port 9559, in mgmtVrf VRF
SSL profile: campus
Authentication username priority: x509-spiffe, x509-common-name
Total clients: 0
Accounting requests: no
```

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>show management security ssl profile campus detail
Profile: campus
State: valid
Trusted certificates: n/a
```

3. mTLS mode(p4-runtime is enabled and ssl profile is configured with trusted certificates) + Accounting is enabled for p4-runtime service Or gNSI acctz is enabled + gNSI Authz is disabled

```
switch>show p4-runtime
Enabled: yes
Server: running on port 9559, in mgmtVrf VRF
SSL profile: campus
Authentication username priority: x509-spiffe, x509-common-name
Total clients: 0
Accounting requests: yes
```

```
switch>show management security ssl profile campus detail
Profile: campus
State: valid
Trusted certificates:
        - clientRootCa
```

```
switch>show management api gnsi
Transport: no transport configured
Acctz enabled: yes
Attestz enabled: no
Authz enabled: no
Certz enabled: no
Credentialz enabled: no
Enrollz enabled: no
Pathz enabled: no
```

If P4Runtime is not configured there is no exposure to this issue and the message will look like:

```
switch>show p4-runtime
Enabled: no
```

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.

Indicators of Compromise

There are no specific Indicators of Compromise (IOCs) available for this issue at this time.

Mitigation

To mitigate this issue, it is recommended to configure the p4-runtime service in mTLS mode (ssl profile with trust certificates). Additionally, enable gNSI Authz to facilitate RPC authorization via the client certificate SPIFFE-ID. Please note that enabling mTLS config will terminate all existing P4 client connections and may cause control plane disruption since packetI/O operations are impacted.

Before implementing this solution, the following pre-requisites must be met:

1. Generate SPIFFE-ID client certificate signed by the server trusted CA and use it for establishing P4 client connection to the server.
2. Define a json file with SPIFFE-ID based policies for Authz service and install it on the device using gNSI Authz.Rotate() rpc

```
switch>show running-config section p4-runtime
p4-runtime
   no shutdown
   !
   transport grpc foo
      ssl profile campus
      authentication username priority x509-spiffe
```

```
switch>show running-config section security
management security
   ssl profile campus
      certificate server.crt key server.key
      trust certificate ca.crt
```

```
switch>show running-config section gnsi
management api gnsi
   service authz
```

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.

Detection using CloudVision

An AlertBase rule has been written to detect the impacted systems; affected systems will be listed in the Compliance Dashboard. CVaaS users will have this rule automatically available in their tenants. For on-prem CloudVision clusters, additional data must be streamed to the cluster from EOS devices to enable this rule to detect affected systems.

Using a service account token, issue the following curl command to the primary node of the cluster:

```
curl -sS -kX POST --header 'Accept: application/json' -b access_token=`cat <access_token>` 'https://<cluster node IP>/api/v3/services/tastreaming.TerminattrStreaming/SubscribeTAPaths' -d '}'
```

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-2026-73453 has been fixed in the following releases:

- 4.36.2F and later releases in the 4.36.x train
- 4.35.6M and later releases in the 4.35.x train
- 4.34.8M and later releases in the 4.34.x train

Hotfix

There is no hotfix 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

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.