Date: June 23, 2026

Revision	Date	Changes
1.0	June 23, 2026	Initial release

The CVE-ID tracking this issue: CVE-2026-12546
CVSSv3.1 Base Score: 6.0 (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L)
CVSSv4.0 Base Score: 5.1
(CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:N/VI:N/VA:L/SC:L/SI:L/SA:L)
Common Weakness Enumeration: CWE-288: Authentication Bypass Using an Alternate Path or Channel
This vulnerability is being tracked by BUG1359868

Description

On affected platforms running Arista EOS (Extensible Operating System) configured with next-hop redirection features—such as Policy-Based Routing (PBR), Border Gateway Protocol (BGP) Flowspec, Traffic Policy, DirectFlow, or Segment Security—certain specific classes of IP packets requiring exception handling may bypass the configured redirection action. Instead of being redirected to the designated next hop, these packets may be handled via fallback software forwarding paths, which can result in the packets being routed according to the system's standard forwarding information.

Risk Profile: Inherent attack complexity is high. To trigger this behavior, packets matching an active redirection policy must meet distinct processing exception criteria. If successfully exploited, this issue could lead to a localized bypass of the intended redirection policy or localized CPU overhead. This vulnerability does not allow for arbitrary code execution, privilege escalation, or unauthorized access to the device.

This issue was discovered internally by Arista and we are not aware of any malicious uses of this issue in customer networks.

Vulnerability Assessment

Affected Software

Policy Based Routing (PBR)

EOS Versions

- 4.36.0.1F and below releases in the 4.36.x train
- 4.35.3M and below releases in the 4.35.x train
- 4.34.5M and below releases in the 4.34.x train
- 4.33.7M and below releases in the 4.33.x train

- 4.32.10M and below releases in the 4.32.x train

BGP Flowspec

EOS Versions

- 4.36.0.1F and below releases in the 4.36.x train
- 4.35.3M and below releases in the 4.35.x train
- 4.34.5M and below releases in the 4.34.x train
- 4.33.7M and below releases in the 4.33.x train
- 4.32.10M and below releases in the 4.32.x train

Traffic Policy

EOS Versions

- 4.36.0.1F and below releases in the 4.36.x train
- 4.35.3M and below releases in the 4.35.x train
- 4.34.5M and below releases in the 4.34.x train
- 4.33.7M and below releases in the 4.33.x train
- 4.32.10M and below releases in the 4.32.x train

Direct Flow

EOS Versions

- 4.36.0.1F and below releases in the 4.36.x train
- 4.35.3M and below releases in the 4.35.x train
- 4.34.5M and below releases in the 4.34.x train
- 4.33.7M and below releases in the 4.33.x train
- 4.32.10M and below releases in the 4.32.x train

Segment Security

EOS Versions

- 4.35.3M and below releases in the 4.35.x train
- 4.34.5M and below releases in the 4.34.x train
- 4.33.7M and below releases in the 4.33.x train
- 4.32.10M and below releases in the 4.32.x train

Affected Platforms

Policy Based Routing (PBR)

The following products are affected by this vulnerability when policy-based routing (PBR) is configured:

- Arista EOS-based products:
  - 720XP/722XPM Series
  - 7010 Series
  - 7010X Series
  - 7020R Series
  - 7160 Series
  - 7050X/X2/X3/X4 Series
  - 7060X/X2/X4/X5/X6 Series
  - 7250X Series
  - 7260X/X3 Series
  - 7280E/R/R2/R3 Series
  - 7300X/X3 Series
  - 7320X Series
  - 7358X4 Series
  - 7368X4 Series
  - 7388X5 Series
  - 7500E/R/R2/R3 Series
  - 7800R3/R4 Series

BGP Flowspec

The following products are affected by this vulnerability when BGP Flowspec is configured:

- Arista EOS-based products:
  - 7020R Series
  - 7280E/R/R2/R3 Series
  - 7500E/R/R2/R3 Series
  - 7800R3/R4 Series

Traffic Policy

The following products are affected by this vulnerability when Traffic Policy is configured:

- Arista EOS-based products:
  - 720D Series
  - 720XP/722XPM Series
  - 750 Series
  - 7010TX Series

- 7020R Series
- 7050X3/X4 Series
- 7060X5/X6 Series
- 7280E/R/R2/R3/R4 Series
- 7300X/X3 Series
- 7358X4 Series
- 7388X5 Series
- 7500E/R/R2/R3 Series
- 7800R3/R4 Series

DirectFlow

The following products are affected by this vulnerability when DirectFlow is configured:

- Arista EOS-based products:
  - 720XP
  - 750 Series
  - 7010TX Series
  - 7050X3/X4 Series
  - 7060X5/X6 Series
  - 7250X Series
  - 7260X/X3 Series
  - 7300X/X3 Series
  - 7320X Series
  - 7368X4 Series

Segment Security

The following products are affected by this vulnerability when Segment Security is configured:

- Arista EOS-based products:
  - 720D Series
  - 720XP/722XPM Series
  - 750 Series
  - 7010TX Series
  - 7050X3 Series
  - 7300X3 Series
  - 7280R3 Series
  - 7500R3 Series
  - 7800R3 Series

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

- Arista EOS-based products:
    - 710 Series
    - 7130 Series running EOS
    - 7150 Series
    - 7170 Series
    - 7700R4 Series
    - AWE 5000 Series
    - AWE 7200R Series
    - CloudEOS
    - cEOS-lab
    - vEOS-lab
    - CloudVision eXchange, virtual or physical appliance
- Arista Wireless Access Points
- CloudVision CUE, virtual appliance or physical appliance
- CloudVision CUE cloud service delivery
- CloudVision Portal, virtual appliance or physical appliance
- CloudVision as-a-Service
- CloudVision AGNI
- Arista 7130 Systems running MOS
- Arista Converged Cloud Fabric (formerly Big Switch BCF)
- Arista DANZ Monitoring Fabric (formerly Big Switch BMF)
- 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)

Note: If you do not see a product listed above, please review the End of Software Support list (here).

Required Configuration for Exploitation

In order to be vulnerable to CVE-2026-12546, one of the following 5 conditions must be met:

Policy Based Routing (PBR)

```
switch(config)#show policy-map type pbr
Service policy pmap1
  Configured on: Ethernet20/1
  Applied on:    Ethernet20/1
  10: Single match statement
    Match:
```

```
        0 permit ip any host 10.2.1.1
    Configured actions: set nexthop 10.20.1.1
    Active routing action:
    VRF default
        Route to nexthop 10.20.1.1 default
```

PBR needs to be configured with a nexthop action and MTU exceeding packets need to be sent matching the rule.

BGP Flowspec
OR

```
switch#show flow-spec ipv4
Flow specification rules for VRF default
Configured on: Ethernet20/1
Applied on: Ethernet20/1
  Flow-spec rule: 10.100.0.0/16;*;
    Rule identifier: 1
    Matches:
      Destination prefix: 10.100.0.0/16
    Actions:
      Redirect: VRF default
                Route via next hop 10.20.4.1
    Status:
      Installed: yes
      Counter: 0 packets, 0 bytes
```

BGP Flowspec needs to be configured with a redirect action and MTU exceeding packets need to be sent matching the rule.

Traffic Policy
OR

```
switch#show traffic-policy interface
Traffic policy foo
   Configured on input of interfaces: Ethernet20/1
   Applied on input of interfaces for IPv4 traffic: Ethernet20/1
   Applied on input of interfaces for IPv6 traffic:
   Applied on input of interfaces for MAC traffic:
   Configured on output of interfaces:
   Applied on output of interfaces for IPv4 traffic:
   Applied on output of interfaces for IPv6 traffic:
```

```
   Total number of rules configured: 3
      match rule1 ipv4
         Destination prefix: 10.100.0.0/16
         Actions: Redirect next hop 10.20.4.1
                      Active routing action:
                      VRF default
                          Route via next hop 10.20.4.1 VRF default
      match ipv4-all-default ipv4
      match ipv6-all-default ipv6
```

Traffic Policy needs to be configured with a nexthop action and MTU exceeding packets need to be sent matching the Traffic Policy rule.

DirectFlow
OR

```
switch(config)#show directflow detail
Flow flow-nexthop: (Flow programmed)
  persistent: True
  installation: True
  priority: 0
  priorityGroupType: default
  hard timeout: 0
  idle timeout: 0
  match:
    Ethernet type: IPv4
    source IPv4 address: X.Y.W.X/255.255.255.255
  actions:
    output nexthop: Y.Z.W.X
  source: config
  matched: 0 packets, 0 bytes
Flows: 1 programmed, 0 rejected
switch(config)#
```

Directflow needs to be configured with a nexthop action and MTU exceeding packets need to be sent matching the flow.

Segment Security
OR

```
switch(config)#show segment-security policy
policy: p1
```

```
   10 application app1 action redirect next-hop 12.2.2.1 stateless
policy: policy-drop-all [readonly]
   10 application app-match-all action drop stateless
policy: policy-forward-all [readonly]
   10 application app-match-all action forward stateless
switch(config)#
```

Indicators of Compromise

There are no distinct systemic Indicators of Compromise (IOCs) available to identify historical exploitation of this issue. Elevated CPU utilization tracking to kernel software forwarding paths or unexpected security-policy bypass matching MTU-exceeding traffic may indicate a vulnerable state.

Mitigation

For all affected systems, the suggested mitigation for all five affected features is to drop all IPv4 MTU exceeding traffic via the ***ip software forwarding mtu exceed action drop*** command, available in 4.36.1F and later releases in the 4.36 train, 4.35.4M and later releases in the 4.35 train, 4.34.6M and later releases in the 4.34 train, 4.33.8M and later releases in the 4.33 train and 4.32.11M and later releases in the 4.32 train.

The command installs an iptables rule that drops all IPv4 packets exceeding the MTU size traffic in the filter table of the FORWARD chain.

Caution: Applying this mitigation causes the switch to drop packets that exceed the interface MTU rather than fragmenting or slow-path forwarding them. Ensure that Path MTU Discovery (PMTUD) is functioning correctly within your network, or verify that end-hosts do not rely on network devices to fragment traffic, as dropping these packets may result in localized data loss or broken applications.

```
# Configure the size of the MTU of the packet for checking. 1500 is the default size
switch(config)#ip software forwarding mtu 1500

# Create iptable rule to drop MTU exceeding packets
switch(config)#ip software forwarding mtu exceed action drop

# Below is shown to illustrate what the rule does. This is not a command that needs t
o be run.
switch(config)#bash sudo iptables -vnL EOS_FORWARD
Chain EOS_FORWARD (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0
```

```
    length 1501:65535
    0     0 REJECT     all  --  *      fwd+    0.0.0.0/0            0.0.0.0/0
    u32 ! "0x0>>0x18=0x45" reject-with icmp-admin-prohibited
    0     0 DROP       all  --  *      ma+     0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     all  --  *      *      !127.0.0.0/8         !127.0.0.0/8
switch(config)#
```

Resolution

The recommended resolution is to upgrade to a remediated software version that contains the ***ip software forwarding mtu*** CLI command, and configure the command 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-2026-12546 has been fixed in the following releases:

- 4.36.1F and later release in the 4.36.x train
- 4.35.4M and later release in the 4.35.x train
- 4.34.6M and later release in the 4.34.x train
- 4.33.8M and later release in the 4.33.x train
- 4.32.11M and later release in the 4.32.x train

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