

Date: October 29, 2024

Revision	Date	Changes
1.0	October 29, 2024	Initial release

Description

Multiple vulnerabilities exist for the Arista Edge Threat Management - Arista NG Firewall (NGFW):

1) **Description**: A user with administrator privileges can perform command injection CVE: CVE-2024-9131 (ZDI-CAN-24015)

CVSSv3.1 Base Score: 7.2 (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H) Common Weakness Enumeration: CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')

This vulnerability is being tracked by NGFW-14800

2) Description: The administrator is able to configure an insecure captive portal script **CVE**: CVE-2024-9132 (ZDI-CAN-24019)

CVSSv3.1 Base Score: 8.1 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H) Common Weakness Enumeration: CWE-94: Improper Control of Generation of Code ('Code Injection')

This vulnerability is being tracked by NGFW-14744

3) **Description**: A user with administrator privileges is able to retrieve authentication tokens **CVE**: CVE-2024-9133 (ZDI-CAN-24324)

CVSSv3.1 Base Score: 6.6 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L) Common Weakness Enumeration: CWE-287: Improper Authentication This vulnerability is being tracked by NGFW-14800

4) Description: Multiple SQL Injection vulnerabilities exist in the reporting application. A user with advanced report application access rights can exploit the SQL injection, allowing them to execute commands on the underlying operating system with elevated privileges. CVE: CVE-2024-9134 (ZDI-CAN-24325)

CVSSv3.1 Base Score: 8.3 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L) Common Weakness Enumeration: CWE-89: Improper Neutralization of Special Elements used in an SQL Command

This vulnerability is being tracked by NGFW-14721

5) **Description**: Expired and unusable administrator authentication tokens can be revealed by units that have timed out from ETM access CVE: CVE-2024-47517 CVSSv3.1 Base Score: 6.8 (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:L/A:L) **Common Weakness Enumeration:** CWE-1230: Exposure of Sensitive Information Through Metadata



This vulnerability is being tracked by NGFW-14754

6) **Description**: Specially constructed queries targeting ETM could discover active remote access sessions

CVE: CVE-2024-47518

CVSSv3.1 Base Score: 6.4 (CVSS:3.1AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/) **Common Weakness Enumeration:** CWE-552: Files or Directories Accessible to External Parties

This vulnerability is being tracked by NGFW-14626

 7) Description: Backup uploads to ETM subject to man-in-the-middle interception
 CVE: CVE-2024-47519 CVSSv3.1 Base Score: 8.3 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L)
 Common Weakness Enumeration: CWE-322: Key Exchange without Entity Authentication This vulnerability is being tracked by NGFW-14708

8) Description: A user with advanced report application access rights can perform actions for which they are not authorized
CVE: CVE-2024-47520
CVSSv3.1 Base Score: 7.6 (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:L)
Common Weakness Enumeration: CWE-653: Improper Isolation or Compartmentalization This vulnerability is being tracked by NGFW-14707

9) Description: Specially constructed queries cause cross platform scripting leaking administrator tokens
CVE: CVE-2024-9188 (ZDI-CAN-24407)
CVSSv3.1 Base Score: 8.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)
Common Weakness Enumeration: unknown
This vulnerability is being tracked by NGFW-14822

Arista would like to acknowledge and thank Mehmet INCE from PRODAFT.com, working with Trend Micro's Zero Day Initiative for responsibly reporting CVE-2024-9131, CVE-2024-9132, CVE-2024-9133, CVE-2024-9134, CVE-2024-47517, CVE-2024-47519, CVE-2024-47520, and CVE-2024-47521.

We would also like to acknowledge and thank Gereon Huppertz, working with Trend Micro's Zero Day Initiative for responsibly reporting CVE-2024-9188

Vulnerability Assessment

Affected Software

- Arista Edge Threat Management Arista NG Firewall Versions
 - 17.1.1 and prior

Copyright 2025 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.



Affected Platforms

• Arista Edge Threat Management - Arista NG Firewall (Formerly Untangle)

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
 - 7010 Series
 - 7010X Series
 - 7020R Series
 - 7130 Series running EOS
 - 7150 Series
 - 7160 Series
 - 7170 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
 - 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 and DANZ Monitoring Fabric (Formerly Big Switch



Nodes for BCF and BMF)

- Arista Network Detection and Response (NDR) Security Platform (Formerly Awake NDR)
- Arista NetVisor OS, Arista NetVisor UNUM, and Insight Analytics (Formerly Pluribus)

Required Configuration for Exploitation, Indicators of Compromise and Mitigation Options

To determine if you are vulnerable to and to mitigate, see the following:

1) CVE-2024-9131 (ZDI-CAN-24015) - A user with administrator privileges can perform command injection

Required Configuration for Exploitation

No required configuration.

Indicators of Compromise

Any compromise will reveal itself via unapproved processes, A typical unapproved process might be an a reverse shell attempt that could look like the following:

ps awwwux | grep [n]vlp root 23100 0.0 0.0 2464 1784 pts/1 S+ 12:02 0:00 nc -nvlp 1337

Mitigation

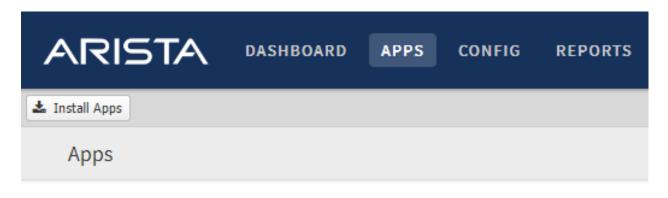
No known mitigation.

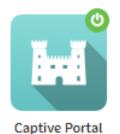
2) CVE-2024-9132 (ZDI-CAN-24019) - The administrator is able to configure an insecure captive portal script

Required Configuration for Exploitation

1. As the NGFW administrator, log into the user interface and navigate to the Apps and Services page.







- 2. If you do not see the Captive Portal application, it is not installed and the system is not
- 3. vulnerable.
- 4. Click the Captive Portal application
- 5. If you see the status that **Captive Portal is disabled**, the system is not vulnerable.

ARISTA »	ASHBOARD	APPS	CONFIG	REPORTS	SESSIONS	HOSTS	DEVICES	USERS	Ŷ	Ø	0
O Back to Apps (Default)	ptive Portal 🔵										
Status Capture Rules Pass	ed Hosts Capt	tive Page	User Authen	itication							
Sessions		ف Powe	Captivo	Portal allows administ rk usage policy, before a	rators to require netwo	rk users to co	omplete a defir	ed process, such	n as logging	in or acce	pting
11:51:00 11:51:3	0 11:52:00		Captive Porta	al is disabled.							
Current Sessions	0	— 🕒 Repo	e et e								
Current TCP Sessions	0	- Griepe	0115								
Current UDP Sessions	0										
DNS Lookups	0										
Login Failure	0										
Login Success	0										
Session Requests	37										
Sessions	0										
Sessions Allowed	37										
Sessions Blocked	0										
TCP AppSession Requests	3										
TCP Sessions	0										
UDP AppSession Requests	34										
UDP Sessions	0										

- 6. Click the Captive Page tab.
- 7. If the Custom radio button is not selected, the system is not vulnerable.



ARISTA DASHBOARD APPS CONFIG REPORTS SESSIONS HOSTS DEVICES USERS 8	0
O Back to Apps (Default Policy) Captive Portal O	
Status Capture Rules Passed Hosts Captive Page User Authentication 🖮 View Reports	
Basic Message Basic Login Image: Custom Preview Captive Portal Page Captive Portal Page Configuration	
Upload Custom Captive Page ZIP File Active Custom File:	
Remove Custom File	
Session Redirect	
Block instead of capture and redirect unauthenticated HTTPS connections	
I Use hostname instead of IP address for the capture page redirect	
Always use HTTPS for the capture page redirect	
Redirect URL:	
NOTE: The Redirect URL field must start with http:// or https:// and allows you to specify a page to display immediately after user authentication. If you leave this field blank, users will instead forwarded to their original destination.	d be

An example of a vulnerable page (The "Custom" radio button is selected)

Indicators of Compromise

Any compromise will reveal itself via unapproved processes. A typical unapproved process might be an a reverse shell attempt that could look like the following:

```
# ps awwwux | grep [n]vlp
root 23100 0.0 0.0 2464 1784 pts/1 S+ 12:02 0:00 nc -nvlp 1337
```

Mitigation

Disable custom page.

- 1. As the NGFW administrator, log into the UI and navigate to the Captive Portal application.
- 2. Select either "Basic Message" or "Basic Login"
- 3. Click Save.

3) CVE-2024-9133 (ZDI-CAN-24324) - A user with administrator privileges is able to retrieve authentication tokens

Required Configuration for Exploitation

No required configuration.



Indicators of Compromise

Any compromise will reveal itself via unapproved processes, A typical unapproved process might be an a reverse shell attempt that could look like the following:

ps awwwux | grep [n]vlp root 23100 0.0 0.0 2464 1784 pts/1 S+ 12:02 0:00 nc -nvlp 1337

Mitigation

No known mitigation.

4) CVE-2024-9134 (ZDI-CAN-24325) - Multiple SQL Injection vulnerabilities exist in the reporting application.

Required Configuration for Exploitation

If the NGFW has one or more Report application Report Users with Online Access enabled they are vulnerable.

To access this information:

1. As the NGFW administrator, log into the UI and navigate to the Reports application.

ARISTA	Ν					Ŷ	(9)	by Pain
O Back to Apps (Default I	Policy) 🚹	Reports 🔵		9770				
Status All Reports	Data Em	ail Templates	Reports Users	Name Map				
Reports Users are user	s that can vi	ew reports and	receive email re	eports but do not have	administration privile		Import	↑ Export
Email Address (username)	Email Alerts	Email Reports	Email Templates		Online Access	Change Password	Edit	Delete
admin			Reports	and the Paris St		A	ø	8
reportuser@domain.com			Reports			a	ø	8

The above picture shows the configuration panel for user access. The "reportuser@domain.com" user has "Online Access" checked, which is required in order to be vulnerable.

Indicators of Compromise

Any compromise will reveal itself via the postgres user running a non-standard postgres process.

Copyright 2025 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.



For example, an appropriate process list for running the postgres database will look like:

```
# ps -u postgres -f
UID
           PID
                PPID C STIME TTY
                                           TIME CMD
postgres 94057
                                        00:00:00 /usr/lib/postgresql/13/bin/postgres
                    1 0 Feb06 ?
-D /var/lib/postgresql/13/main -c config_file=/etc/postgresql/13/main/postgresql.con
f
                                        00:00:02 postgres: 13/main: checkpointer
postgres 94063 94057 0 Feb06 ?
postgres 94064 94057 0 Feb06 ?
                                        00:00:00 postgres: 13/main: background write
r
postgres 94065 94057 0 Feb06 ?
                                        00:00:12 postgres: 13/main: walwriter
postgres 94066 94057 0 Feb06 ?
                                        00:00:00 postgres: 13/main: autovacuum launc
her
postgres 94067 94057 0 Feb06 ?
                                        00:00:01 postgres: 13/main: stats collector
postgres 94068 94057 0 Feb06 ?
                                        00:00:00 postgres: 13/main: logical replicat
ion launcher
```

Additional processes run by the postgres user indicating a potential compromise may look like:

postgres 100172 100171 0 Feb06 pts/2 00:00:00 bash

Mitigation

For the Reports application, for all Reports Users, disable Online Access.

ARISTA	N					Ŷ	C 🕜 od t	y Paint
O Back to Apps (Default	Policy) 🔝 R	leports 🔵		9773				
Status All Reports	Data Ema	il Templates	Reports Users	Name Map				
Reports Users are user	s that can vie	w reports and	receive email re	eports but do not have	administration privile			
O Add							Import	↑ Export
Email Address (username)	Email Alerts	Email Reports	Email Templates		Online Access	Change Password	Edit	Delete
admin			Reports			a	and the second s	ê
reportuser@domain.com			Reports				ø	ê

To do this:

- 1. As the NGFW administrator, log into the UI and go to the Reports application.
- 2. For all users with the Online Access checkbox (red box) enabled, uncheck it.
- 3. Click Save.



5) CVE-2024-47517 - Expired and unusable administrator authentication tokens can be revealed by units that have timed out from Edge Threat Management (ETM) access

Required Configuration for Exploitation

- 1. Log into Edge Threat Management (ETM).
- 2. Go to Appliances, and click your target NGFW.
- 3. On the NGFW appliance page, click Remote Access.

=	ARISTA Edge Thread Management		GET STARTED 🗸 🥑 🗸 😝 🧸
	DASHBOARD	Q o arista.example.com	Label not assigned • NGFW 17.1.1 • 162.210.129.5 - ADD APPLIANC
▲	ALERTS V	APPLIANCES > APPLIANCE DETAILS	
■	APPLIANCES A	arista.cxample.com - Label Not Set	
	APPLIANCES	Image: Construction of the sector of the	
	NETWORKS	Information	E Appliance Model Custom
	NGFW TEMPLATES	arista.example.com Version: 17.1.1	
	MICRO EDGE POLICIES	ty Up Time: 50h 10m 28s	
	MICRO EDGE TEMPLATES	CPU Count: 1	
	BACKUPS	Architecture: x86_64 Host Count: 1	

- 4. With the NGFW UI in a new tab or window, let the connection expire.
- 5. After the session has expired, any attempt to perform actions will notify you of the need to enable Remote Access again.

Indicators of Compromise

A specially crafted script pointing to the IP port used by the now expired connection will show recurring queries from the UI.

Mitigation

After you have completed NGFW operations with Remote Access, close the browser window or tab.

6) CVE-2024-47518 - Specially constructed queries targeting Edge Threat Management (ETM) could discover active remote access sessions

Required Configuration for Exploitation

- 1. Log into Edge Threat Management (ETM).
- 2. Go to Appliances, and click your target NGFW.
- 3. On the NGFW appliance page, click Remote Access.



≡	ARISTA Edge Tread Management		CET STARTED V 🔮 V 😝 V
	DASHBOARD	Q 😑 arista.example.com	Label not assigned • NGFW 17.1.1 • 162.210.129.5 👻 ADD APPLIANCE
▲	ALERTS 🗸	APPLIANCES > APPLIANCE DETAILS	
	APPLIANCES ^	arista.example.com - Label Not Set	
	APPLIANCES	REMOTE ACCESS UPDATE SOFTWARE C REBOO	$\left(\bigcirc \text{ set label} \right) \left(\textcircled{a} \text{ totp} \right) \left(\textcircled{a} \text{ license} \right) \left(\textcircled{a} \text{ remove} \right)$
	NETWORKS	Information	Appliance Model Custom
	NGFW TEMPLATES	arista.example.com	
	MICRO EDGE POLICIES	Version: 17.1.1 ন্ত Up Time: 50h 10m 28s	
	MICRO EDGE TEMPLATES	1	
	BACKUPS	CPU Count: 1 Architecture: x86_64 Host Count: 1	

4. Leave the connection running.

Indicators of Compromise

- 1. As the NGFW administrator, log into the UI and go to the Reports.
- 2. Under Administration, click Admin Login Events
- 3. Invalid login attempts may appear as failed logins with an "invalid password" reason such as:

ARISTA DASHBOA	ARD AI	PPS CONF	IG RI	EPORTS				
Conditions: O Add - Since: O Today -								
 ▷ ■ Hosts ▷ ■ Devices ▷ ■ Users 		nistration administrator lo		nin Lo	gin Eve	nts	:	C Refresh 🗆 Auto
> 🛃 Network	Q Filter	Search		3 total				
Administration	Timestam)	Login		Local	Client Address	Succeeded	Reason
LIII Admin Logins	2024-09-2	6 05:22:48 pm	admin		remote	192.168.253.10	success	
I Admin Login Events	2024-09-2	6 05:22:45 pm	admin		remote	192.168.253.10	failed	invalid password
i≡ All Settings Changes	2024-09-2	6 05:19:28 pm	admin		remote	192.168.253.10	success	
 O Events O System O Shield 								

Mitigation

After you have completed your Remote Access session, close the NGFW window.

7) CVE-2024-47519 - Backup uploads to ETM subject to man-in-the-middle interception

Required Configuration for Exploitation

1. As the NGFW administrator, log into the user interface and navigate to the Apps and Services page.

Copyright 2025 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.

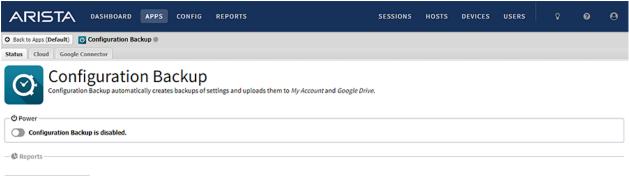


ARISTA	DASHBOARD	APPS	CONFIG	REPORTS
🛓 Install Apps				
Apps				
Service Apps				





- 2. If you do not see the Configuration Backup service application, it is not installed and the system is not vulnerable.
- 3. Click the Configuration Backup application
- 4. If you see the status that **Configuration Backup is disabled**, the system is not vulnerable.



- Remove Configuration Backup
- 5. Click the Cloud tab.
- 6. Click Backup Now.
- 7. Log into Edge Threat Management.
- 8. Go to Appliances and Backups.
- 9. Verify that you see a new backup.



≡	ARISTA Edge Trevel Managament					GET STARTED 🗸	. 0	• • •
-	DASHBOARD		Q 8	Search here			-	ADD APPLIANCE
▲	ALERTS	~	APPLIA	NCES > BACKUPS				
	APPLIANCES	^	Back	kups				
	APPLIANCES							
	NETWORKS							
	NGFW TEMPLATES		Sea	rch here	Showing 4	of 4 total	XPORT CSV	REFRESH
	MICRO EDGE POLICIES		0	Date/Time Sep 24, 2024, 10:06 AM	UID 833f-xxxxxxxxx2762		Download	
	MICRO EDGE TEMPLATES		0	Jul 29, 2024, 7:22 AM	833f-30000000-2762		DOWNLOAD	
	BACKUPS		0	Jun 17, 2024, 12:07 PM	833f-xxxxxxxx2762		DOWNLOAD	
			0	Apr 3, 2024, 10:51 PM	708d-xxxxxxxxx-c762		DOWNLOAD	
₽	HOSTS							
հե	REPORTS	~						
×	TOOLS							
<u>•</u>	DOWNLOAD							
٤	DEV							
20	MY ACCOUNT	~						
	MY ORGANIZATION	~						

Indicators of Compromise

If you do not see a backup in the above list, you may be compromised.

Mitigation

Disable Configuration Backup application.

8) CVE-2024-47520 - A user with advanced report application access rights can perform actions for which they are not authorized

Required Configuration for Exploitation

If the NGFW has one or more Report application Report Users with Online Access enabled they are vulnerable.

To access this information:

1. As the NGFW administrator, log into the UI and navigate to the Reports application.



ARISTA	\		Cri	eated by Paint S		Ŷ	COted	Free T
O Back to Apps (Default I	Policy) 📴 R	leports 🔵		9773				
Status All Reports	Data Ema	il Templates	Reports Users	Name Map				
Reports Users are users	s that can vie	w reports and	receive email re	eports but do not have	administration privile	-	Import	★ Export
Email Address (username)	Email Alerts	Email Reports	Email Templates		Online Access	Change Password	Edit	Delete
admin			Reports		Chille Access		eun	
reportuser@domain.com	E		Reports				de la	8

The above picture shows the configuration panel for user access. The

"reportuser@domain.com" user has "Online Access" checked, which is required in order to be vulnerable.

Indicators of Compromise

- 1. As the NGFW administrator, log into the UI and go to the Reports.
- 2. Under Administration, click All Settings Changes
- 3. Compromised settings for a reportuser@domain.com would appear as:

ARISTA DASHBO	ARD APPS CONF	IG REPORTS			S
Conditions: O Add - Since: O Today -	•				
 Hosts Devices Users 		formed by an administrator.	S	2 Refresh	🗆 Auto (5 sec
> 🔣 Network	Q Filter Search	2 total			
Administration	Timestamp	Settings File	Username	Hostname	Differe
LIII Admin Logins LIII Settings Changes	2024-09-26 05:27:29 pm	untangle-vm/local_directory.js-versio	reportuser@domain.com	192.168.253.10	Q
Admin Login Events	2024-09-26 05:27:27 pm	untangle-vm/system.js-version-2024	reportuser@domain.com	192.168.253.10	Q
I All Settings Changes					
 ▷ ● Events ▷ ● System ▷ ● Shield 					

Mitigation

For the Reports application, for all Reports Users, disable Online Access.



ARISTA	\		Cre	eated by Paint S		Ŷ	C 🔞 sd t	Free Tri
O Back to Apps (Default I	Policy) 🔝 🖪	leports 🔵		0/ 20				
Status All Reports	Data Ema	il Templates	Reports Users	Name Map				
Reports Users are users	s that can vie	w reports and	receive email re	eports but do not have	administration privile		Import	★ Export
Email Address (username)	Email Alerts	Email Reports	Email Templates		Online Access	Change Password	Edit	Delete
admin	V	V	Reports				ø	Û
reportuser@domain.com			Reports				ø	Ê

To do this:

- 1. As the NGFW administrator, log into the UI and go to the Reports application.
- 2. For all users with the Online Access checkbox (red box) enabled, uncheck it.
- 3. Click Save.

9) CVE-2024-9188 (ZDI-CAN-24407) - Specially constructed queries cause cross platform scripting leaking administrator tokens

Required Configuration for Exploitation

No required configuration.

Indicators of Compromise

- 1. As the NGFW administrator, log into the UI and go to the Reports.
- 2. Under Administration, click All Settings Changes
- 3. Compromised settings changes from this exploit would appear from a hostname IP address that you have not logged in from such as:

ARISTA DASHBO	OARD APPS CONF	IG REPORTS			SESSI
Conditions: O Add - Since: O Today	•				
 Hosts M Devices Users 	Administration All settings changes per	S	C Refresh □ Auto (5 sec) 10 10		
▷ 🚮 Network	Q Filter Search 2 total				
A 🖪 Administration	Timestamp	Settings File	Username	Hostname	Differe
LIII Admin Logins	2024-09-26 05:27:29 pm	untangle-vm/local_directory.js-versio	admin	192.168.253.10	Q
E Admin Login Events	2024-09-26 05:27:27 pm	untangle-vm/system.js-version-2024	admin	192.168.253.10	Q

Mitigation

Copyright 2025 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.



No known mitigation.

Resolution

The recommended resolution for all issues documented above is to upgrade to the version indicated below at your earliest convenience.

• 17.2 Upgrade

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