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

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
```

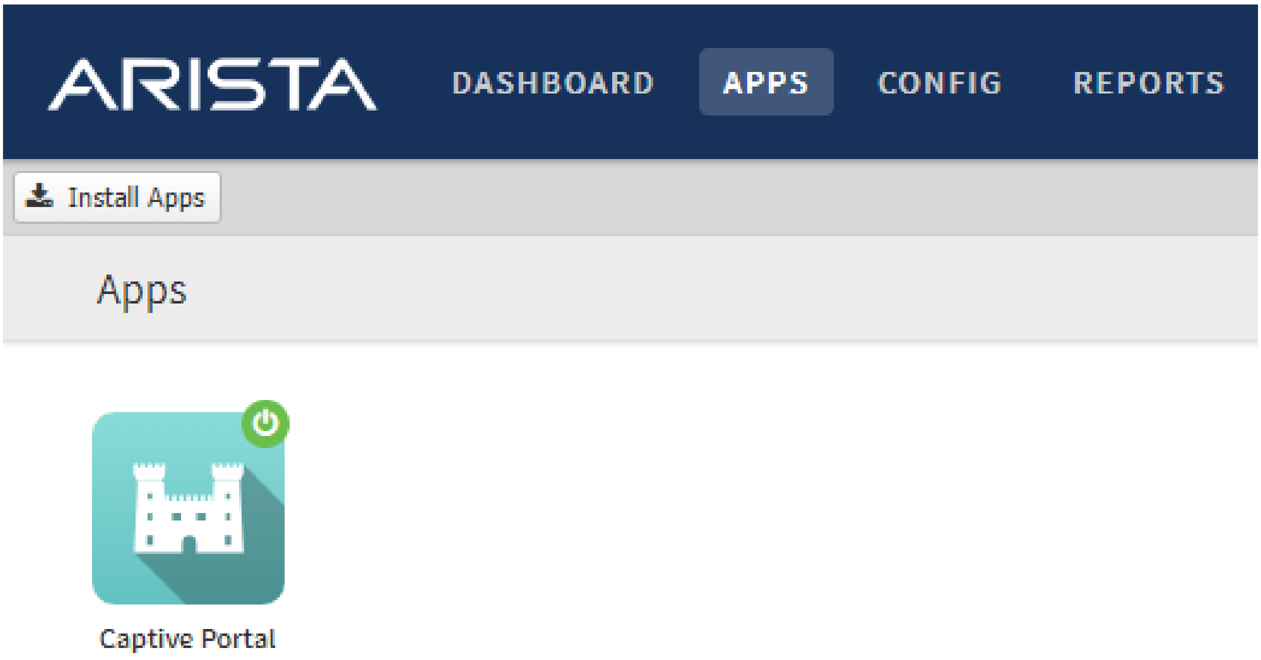
Mitigation

No known mitigation.

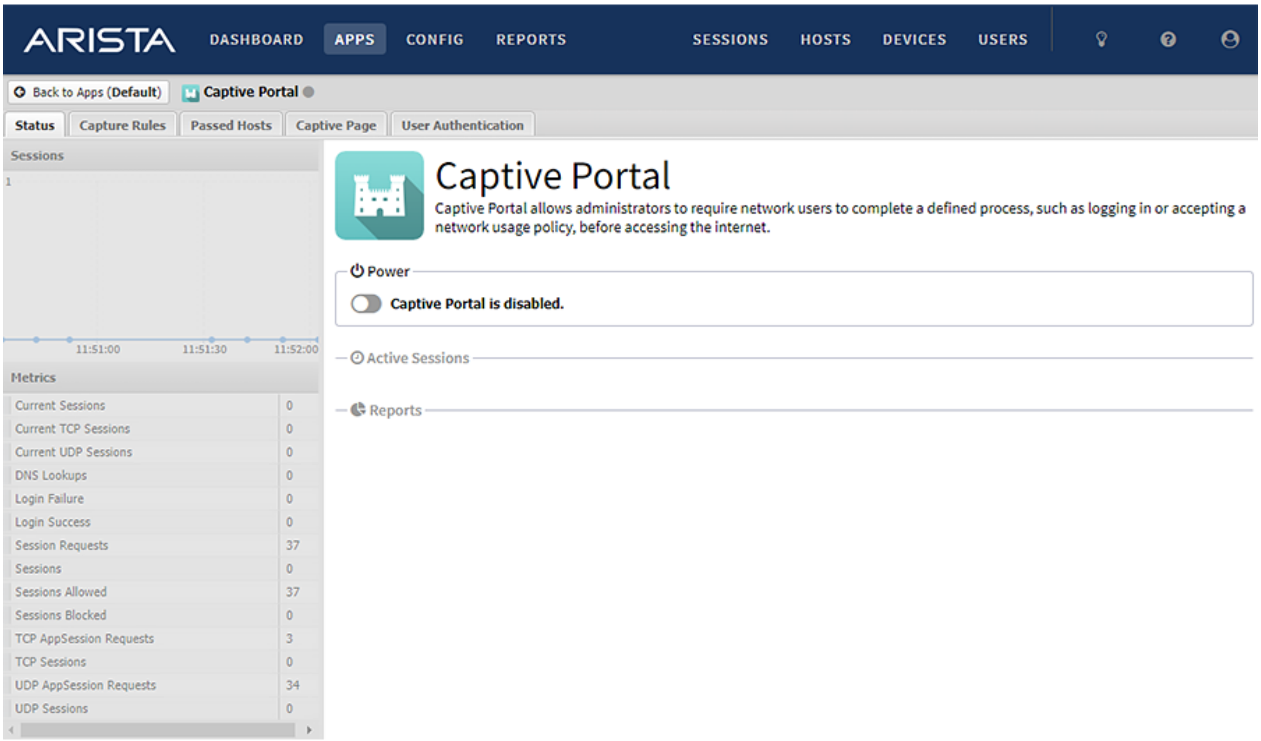
2) CVE-2024-9132 (ZDI-CAN-24019) - The administrator is able to configure an insecure captive portal script

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.



Captive Portal

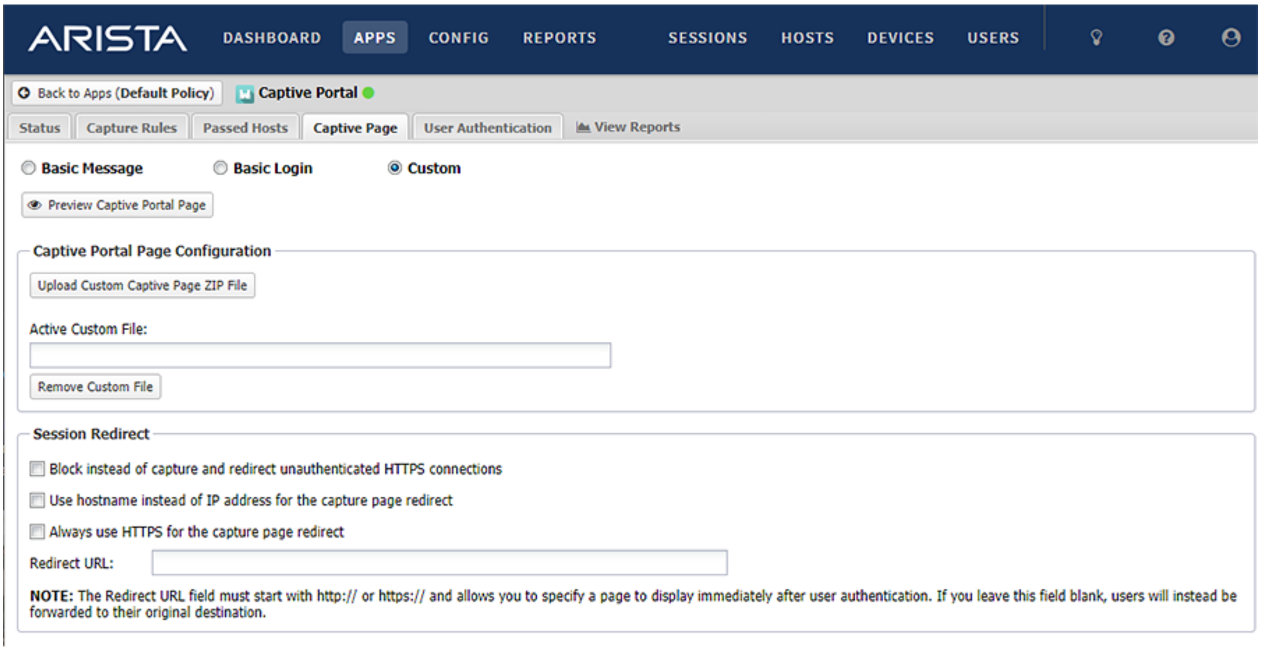
Captive Portal allows administrators to require network users to complete a defined process, such as logging in or accepting a network usage policy, before accessing the internet.

Power

Captive Portal is disabled.

Metrics	
Current Sessions	0
Current TCP Sessions	0
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.



○ Basic Message ○ Basic Login ● Custom

Captive Portal Page Configuration

Active Custom File:

Session Redirect

□ Block instead of capture and redirect unauthenticated HTTPS connections

□ 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 be forwarded to their original destination.

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.

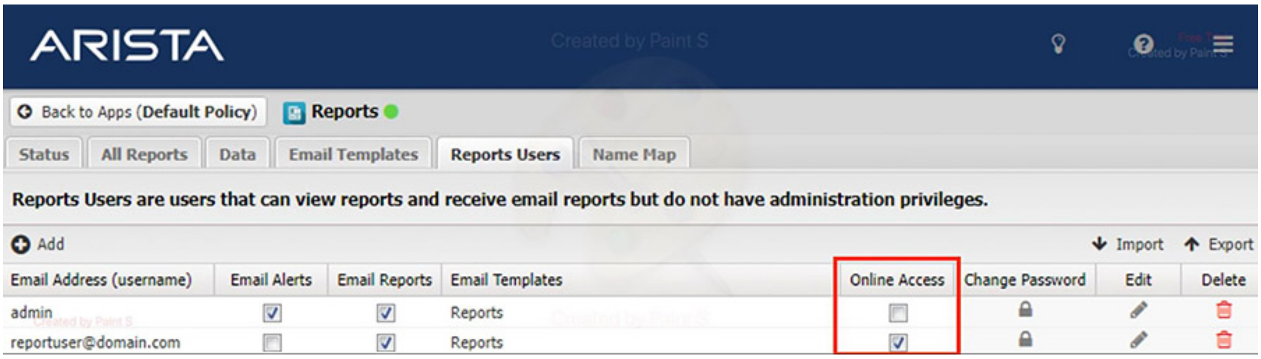
4) CVE-2024-9134 (ZDI-CAN-24325) - Multiple SQL Injection vulnerabilities exist in the reporting application.

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.



Reports Users are users that can view reports and receive email reports but do not have administration privileges.

Email Address (username)	Email Alerts	Email Reports	Email Templates	Online Access	Change Password	Edit	Delete
admin	☑	☑	Reports	□	🔒	✎	🗑
reportuser@domain.com	□	☑	Reports	☑	🔒	✎	🗑

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.

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

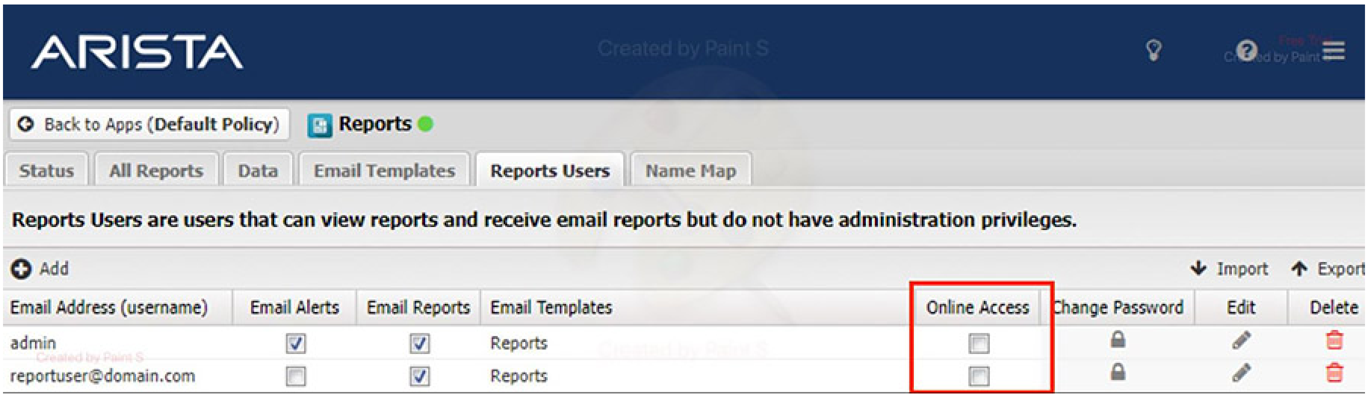
```
# ps -u postgres -f
UID          PID    PPID  C STIME TTY          TIME CMD
postgres  94057       1  0 Feb06 ?        00:00:00 /usr/lib/postgresql/13/bin/postgres
 -D /var/lib/postgresql/13/main -c config_file=/etc/postgresql/13/main/postgresql.con
f
postgres  94063  94057  0 Feb06 ?        00:00:02 postgres: 13/main: checkpointer
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.*



Reports Users are users that can view reports and receive email reports but do not have administration privileges.

Email Address (username)	Email Alerts	Email Reports	Email Templates	Online Access	Change Password	Edit	Delete
admin	☑	☑	Reports	□	🔒	✎	🗑
reportuser@domain.com	□	☑	Reports	□	🔒	✎	🗑

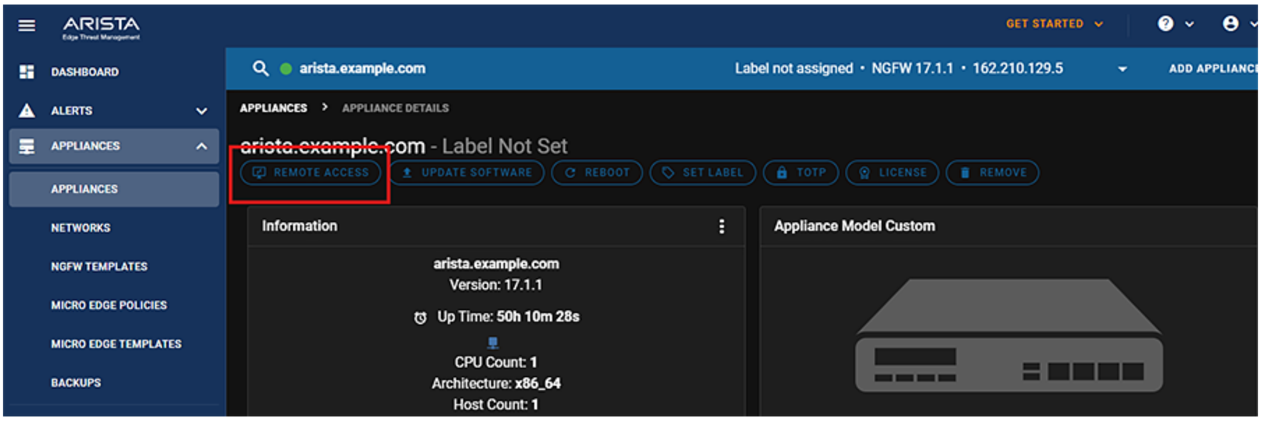
To do this:

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.example.com

Label not assigned • NGFW 17.1.1 • 162.210.129.5

arista.example.com - Label Not Set

arista.example.com
Version: 17.1.1
Up Time: 50h 10m 28s
CPU Count: 1
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.

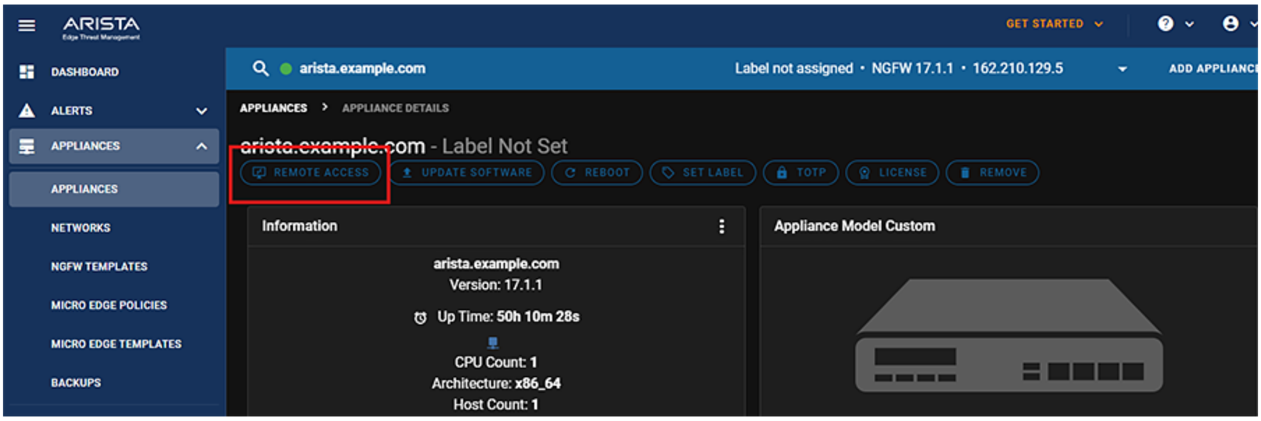
Mitigation

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.example.com · Label not assigned · NGFW 17.1.1 · 162.210.129.5

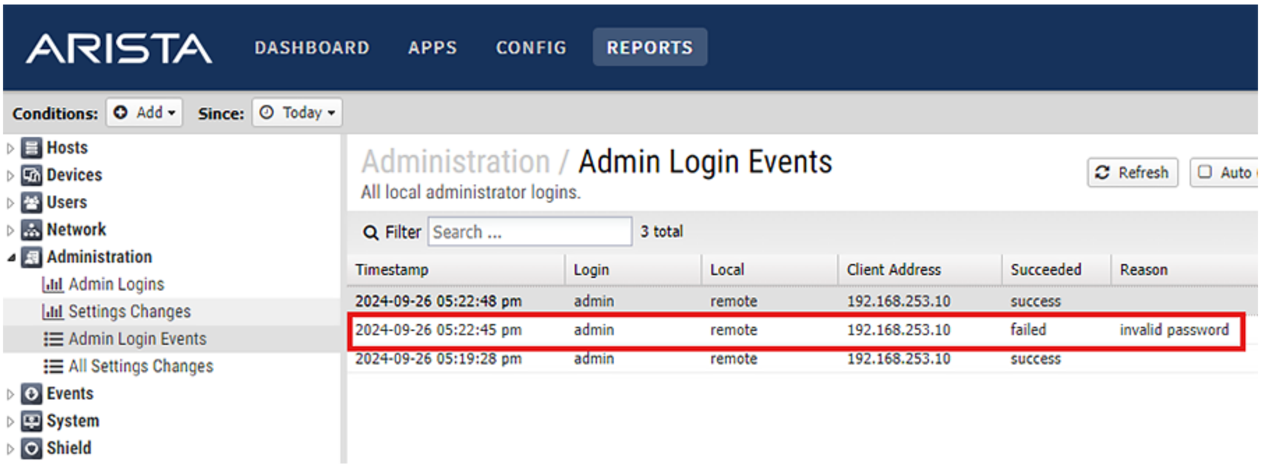
arista.example.com - Label Not Set

arista.example.com
Version: 17.1.1
Up Time: 50h 10m 28s
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:



Administration / Admin Login Events
All local administrator logins.

3 total

Timestamp	Login	Local	Client Address	Succeeded	Reason
2024-09-26 05:22:48 pm	admin	remote	192.168.253.10	success	
2024-09-26 05:22:45 pm	admin	remote	192.168.253.10	failed	invalid password
2024-09-26 05:19:28 pm	admin	remote	192.168.253.10	success	

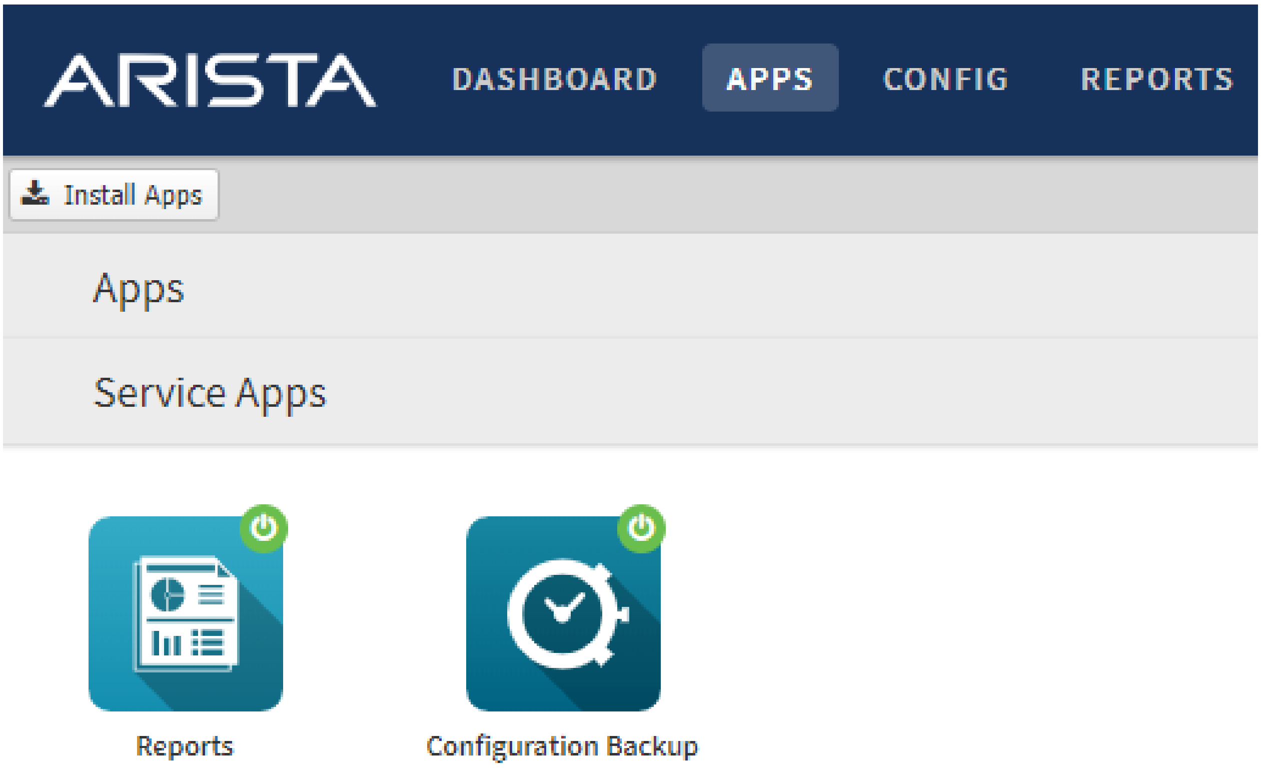
Mitigation

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

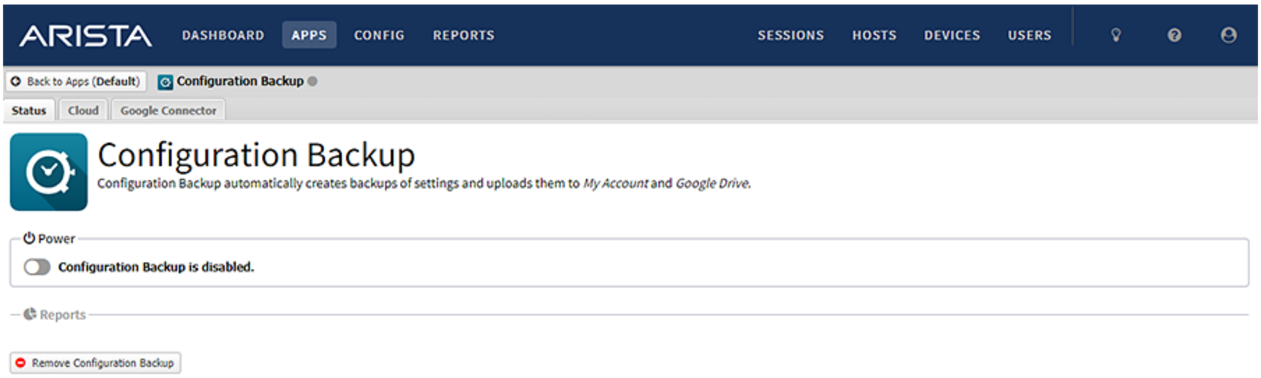
7) CVE-2024-47519 - Backup uploads to ETM subject to man-in-the-middle interception

Required Configuration for Exploitation

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



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.

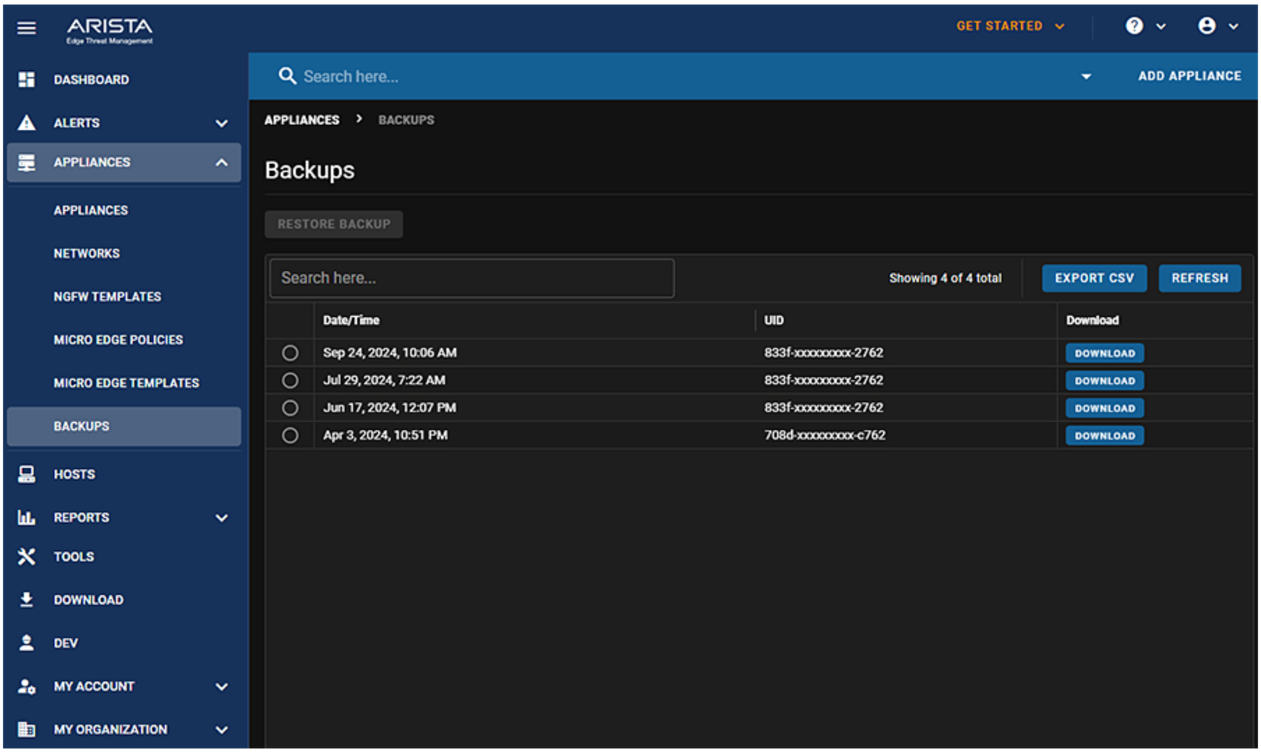


Configuration Backup

Configuration Backup automatically creates backups of settings and uploads them to *My Account* and *Google Drive*.

Configuration Backup is disabled.

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.



	Date/Time	UID	Download
○	Sep 24, 2024, 10:06 AM	833f-xxxxxxxxx-2762	DOWNLOAD
○	Jul 29, 2024, 7:22 AM	833f-xxxxxxxxx-2762	DOWNLOAD
○	Jun 17, 2024, 12:07 PM	833f-xxxxxxxxx-2762	DOWNLOAD
○	Apr 3, 2024, 10:51 PM	708d-xxxxxxxxx-c762	DOWNLOAD

Indicators of Compromise

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

Mitigation

Disable Configuration Backup application.

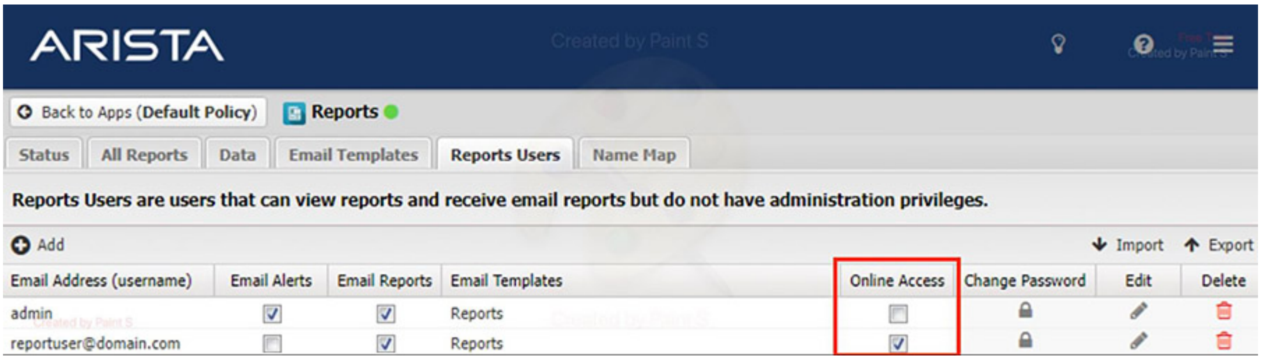
8) CVE-2024-47520 - A user with advanced report application access rights can perform actions for which they are not authorized

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.



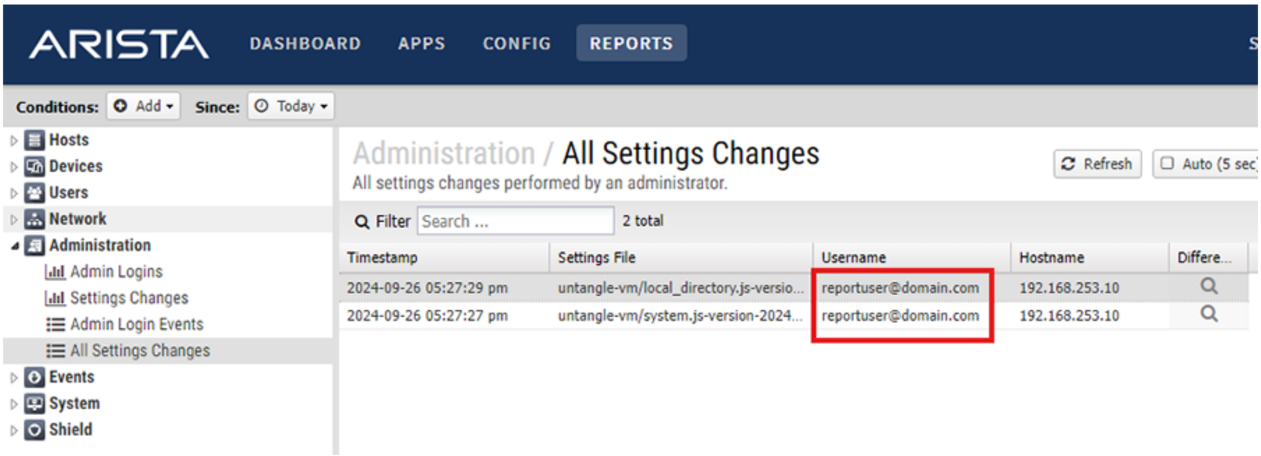
Reports Users are users that can view reports and receive email reports but do not have administration privileges.

Email Address (username)	Email Alerts	Email Reports	Email Templates	Online Access	Change Password	Edit	Delete
admin	☑	☑	Reports	☐			
reportuser@domain.com	☐	☑	Reports	☑			

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:



Administration / All Settings Changes

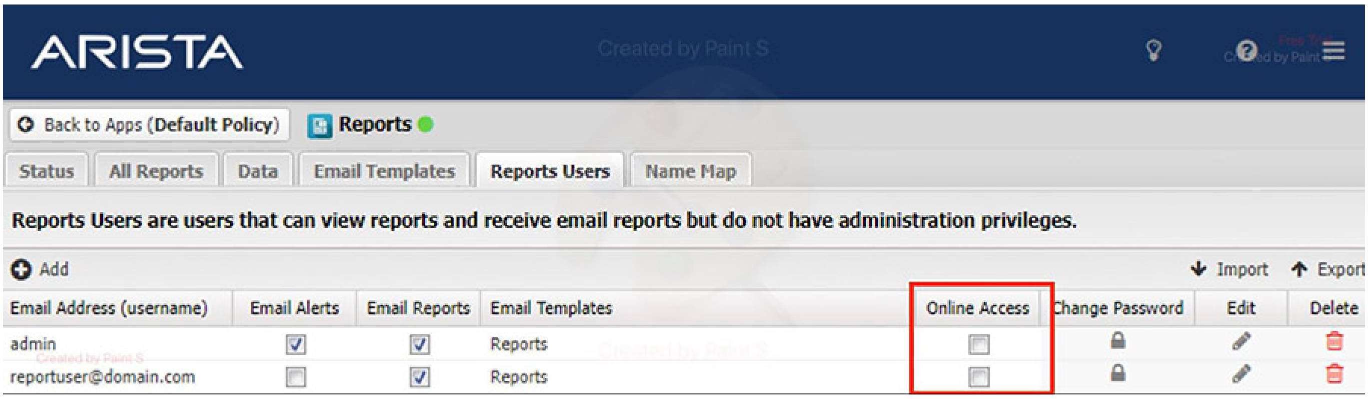
All settings changes performed by an administrator.

2 total

Timestamp	Settings File	Username	Hostname	Differe...
2024-09-26 05:27:29 pm	untangle-vm/local_directory.js-versio...	reportuser@domain.com	192.168.253.10	
2024-09-26 05:27:27 pm	untangle-vm/system.js-version-2024...	reportuser@domain.com	192.168.253.10	

Mitigation

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



Reports Users are users that can view reports and receive email reports but do not have administration privileges.

Email Address (username)	Email Alerts	Email Reports	Email Templates	Online Access	Change Password	Edit	Delete
admin	☑	☑	Reports	□			
reportuser@domain.com	□	☑	Reports	□			

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.

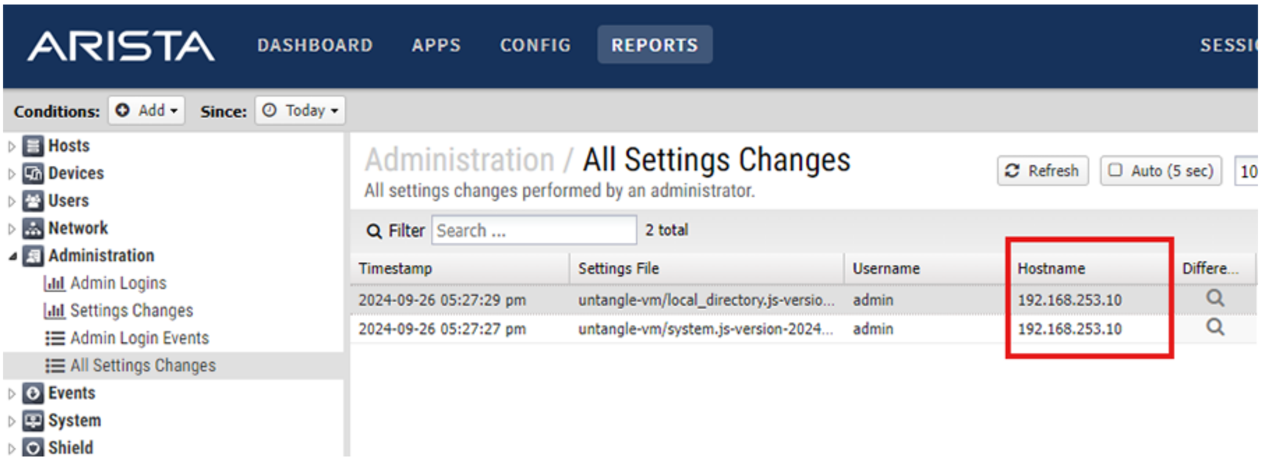
9) CVE-2024-9188 (ZDI-CAN-24407) - Specially constructed queries cause cross platform scripting leaking administrator tokens

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:



Administration / All Settings Changes

All settings changes performed by an administrator.

2 total

Timestamp	Settings File	Username	Hostname	Differe...
2024-09-26 05:27:29 pm	untangle-vm/local_directory.js-versio...	admin	192.168.253.10	
2024-09-26 05:27:27 pm	untangle-vm/system.js-version-2024...	admin	192.168.253.10	

Mitigation

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