Date: October 21, 2025

Revision	Date	Changes
1.0	October 21, 2025	Initial release

Description

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

1) Description: Captive Portal can expose sensitive information
CVE: CVE-2025-6980 (ZDI-CAN-27006)
CVSSv3.1 Base Score: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
Common Weakness Enumeration: CWE-200:
This vulnerability is being tracked by NGFW-15197

2) Description: Captive Portal can allow authentication bypass
CVE: CVE-2025-6979 (ZDI-CAN-27007)
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: CWE-287:
This vulnerability is being tracked by NGFW-15196

3) Description: Diagnostics command injection vulnerability
CVE: CVE-2025-6978 (ZDI-CAN-27310)
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-78:
This vulnerability is being tracked by NGFW-15195

Arista would like to acknowledge and thank Gereon Huppertz working with Trend Zero Day Initiative for reporting ZDI-CAN-27006, ZDI-CAN-27007, and ZDI-CAN-27010.

Vulnerability Assessment

Affected Software

Arista Edge Threat Management - Arista Next Generation Firewall (NGFW) Versions

- 17.3.1 and prior

Affected Platforms

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

- Arista Edge Threat Management - Arista Next Generation Firewall (Formerly Untangle)

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

- Arista EOS-based products:
  - 710/710X 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 Series
  - 7250X Series
  - 7260X/X3 Series
  - 7280E/R/R2/R3/R4 Series
  - 7300X/X3 Series
  - 7320X Series
  - 7358X4 Series
  - 7368X4 Series
  - 7388X5 Series
  - 7500E/R/R2/R3 Series
  - 7800R3/R4 Series
  - CloudEOS
  - cEOS-lab
  - vEOS-lab
  - AWE 5000 Series
- Arista Wireless Access Points
- CloudVision WiFi, virtual appliance or physical appliance
- CloudVision WiFi cloud service delivery
- CloudVision eXchange, virtual or physical appliance
- 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)
- 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, Indicators of Compromise and Mitigation Options

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

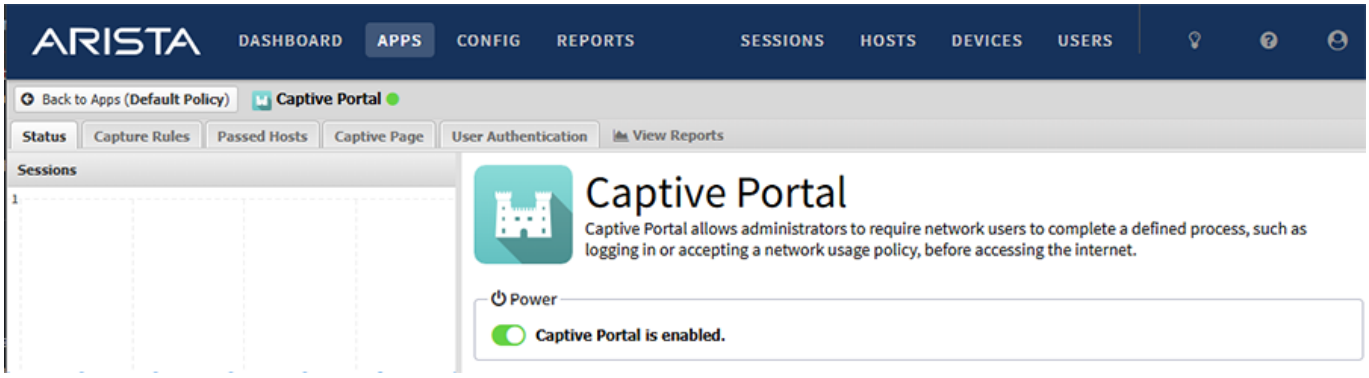
1) CVE-2025-6980 (ZDI-CAN-27006) - Captive Portal can expose sensitive information

Required Configuration for Exploitation

If the Captive Portal application is installed and enabled, the systems are vulnerable.

To access this information:

1. As the NGFW administrator, log into the UI and navigate to the Captive Portal application.
2. If the Captive Portal application is not installed, the system is not vulnerable.
3. If Captive Portal is not enabled, the system is not vulnerable.



The above shows Captive Portal as enabled.

Indicators of Compromise

No evidence of compromise exists.

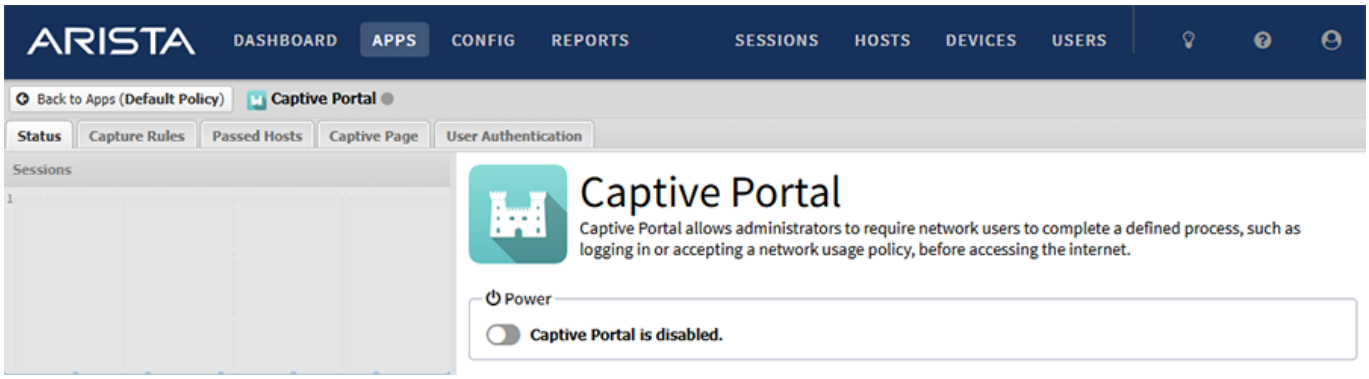
Mitigation

Disable Captive Portal.

As the NGFW administrator, log into the UI and navigate to the Captive Portal application.

1. If the Captive Portal application is not installed, the system is not vulnerable.
2. If Captive Portal is not enabled, the system is not vulnerable.
3. Move the Enabled slider to disabled.
4. Click Save

5. Disable Captive Portal.



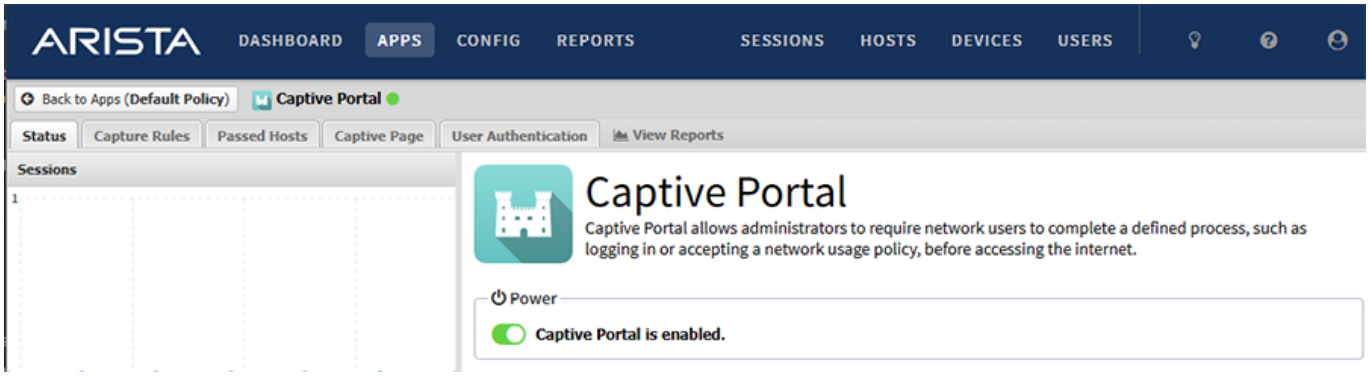
2) CVE-2025-6979 (ZDI-CAN-27007) - Captive Portal can allow authentication bypass

Required Configuration for Exploitation

If the Captive Portal application is installed and enabled, the systems are vulnerable.

To access this information:

1. As the NGFW administrator, log into the UI and navigate to the Captive Portal application.
2. If the Captive Portal application is not installed, the system is not vulnerable.
3. If Captive Portal is not enabled, the system is not vulnerable.



Indicators of Compromise

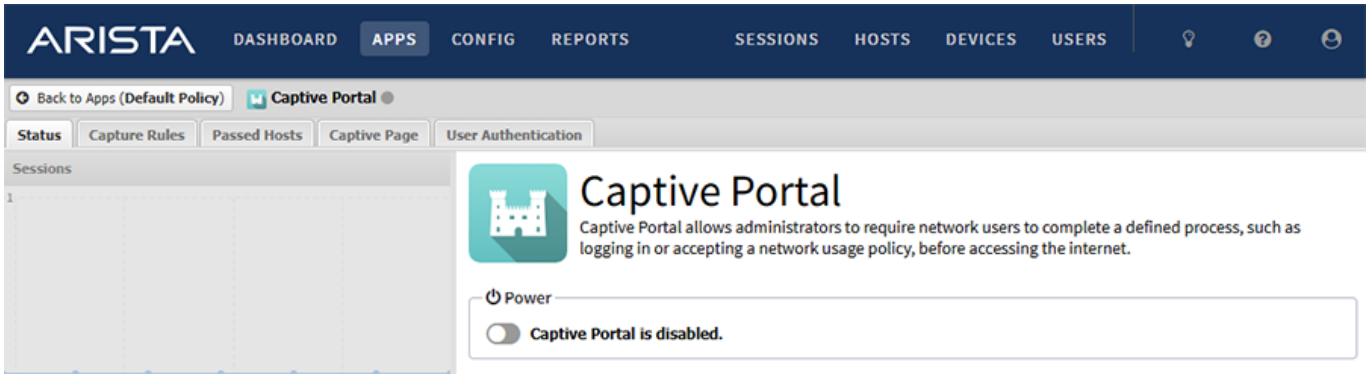
No evidence of compromise exists.

Mitigation

Disable Captive Portal.

As the NGFW administrator, log into the UI and navigate to the Captive Portal application.

1. If the Captive Portal application is not installed, the system is not vulnerable.
2. If Captive Portal is not enabled, the system is not vulnerable.
3. Move the Enabled slider to disabled.
4. Click Save
5. Disable Captive Portal.



3) CVE-2025-6978 (ZDI-CAN-27310) - Diagnostics command injection vulnerability

Required Configuration for Exploitation

1. A successful attack requires administrative access to the NGFW UI.

Indicators of Compromise

No evidence of compromise exists.

Mitigation

Do not allow non-authorized administrative access or access to the administrative browser.

Resolution

The recommended resolution is to upgrade to the version indicated below at your earliest convenience.

- 17.4 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