Date: February 3, 2026

Revision	Date	Changes
1.0	February 3, 2026	Initial release

Description

Several vulnerabilities exist for the Arista Edge Threat Management - Arista NG Firewall (NGFW). On affected platforms, an administrative account logged into the user interface is subject to several command injection vulnerabilities.

1) Description: Administrative diagnostics command injection vulnerability
CVE: CVE-2025-6978
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)
CVSSv4.0 Base Score: 8.6
(CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/S:P)
Common Weakness Enumeration: CWE-78
This vulnerability is being tracked by NGFW-15484

2) Description: Encrypted Password command injection vulnerability
CVE: CVE-2026-25620
CVSSv3.1 Base Score: 6.0 (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:L/A:L)
CVSSv4.0 Base Score: 7.0
(CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:L/VA:L/SC:L/SI:L/SA:L/S:P)
Common Weakness Enumeration: CWE-78
This vulnerability is being tracked by NGFW-15493

3) Description: Reports application vulnerability due to insecure input validation
CVE: CVE-2026-25621
CVSSv3.1 Base Score: 6.0 (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:L/A:L)
CVSSv4.0 Base Score: 7.0
(CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:L/VA:L/SC:L/SI:L/SA:L/S:P)
Common Weakness Enumeration: CWE-78
This vulnerability is being tracked by NGFW-15491

4) Description: Captive Portal Custom Handler command injection vulnerability
CVE: CVE-2026-25622
CVSSv3.1 Base Score: 6.0 (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:L/A:L)
CVSSv4.0 Base Score: 7.0
(CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:L/VA:L/SC:L/SI:L/SA:L/S:P)
Common Weakness Enumeration: CWE-78
This vulnerability is being tracked by /NGFW-15494

5) Description: Command execution vulnerability
CVE: CVE-2026-25623

CVSSv3.1 Base Score: 6.0 (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:L/A:L)
CVSSv4.0 Base Score: 7.0
(CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:L/VA:L/SC:L/SI:L/SA:L/S:P)
Common Weakness Enumeration: CWE-78
This vulnerability is being tracked by NGFW-15490

6) Description: Administrative cross script vulnerability
CVE: CVE-2026-25624
CVSSv3.1 Base Score: 5.7 (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:L/A:L)
CVSSv4.0 Base Score: 5.8
(CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:P/VC:H/VI:L/VA:L/SC:L/SI:L/SA:L/S:P)
Common Weakness Enumeration: CWE-79
This vulnerability is being tracked by NGFW-15492

Arista would like to acknowledge and thank Jon Williams & Ronan Kervella from Bishop Fox for responsibly reporting these issues.

Vulnerability Assessment

Affected Software

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

- 17.4.0 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 /R4Series
  - 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/R4 Series
    - 7300X/X3 Series
    - 7320X Series
    - 7358X4 Series
    - 7368X4 Series
    - 7388X5 Series
    - 7500E/R/R2/R3 Series
    - 7700R4 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 the issue to and for mitigation options, see the following:

1) CVE-2025-6978 - Diagnostics command injection vulnerability

Required Configuration for Exploitation

A successful attack requires administrative access to the NGFW UI.

Indicators of Compromise

No evidence of compromise exists.

Mitigation

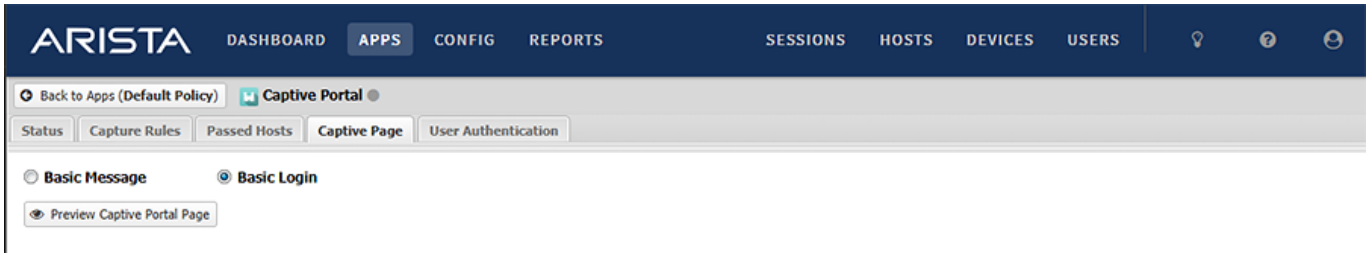
Per operational best practice security models, do not allow unauthorized administrative access to the administrative browser.

2) CVE-2026-25620 - Encrypted Password command injection vulnerability

Required Configuration for Exploitation

Verify the following;

1. An NGFW system, version 17.4.0. Earlier versions are not affected.
2. As the NGFW administrator, log into the UI and navigate to the Captive Portal application.
3. If the Captive Portal application is not installed, the system is not vulnerable.
4. If Captive Portal is not enabled, the system is not vulnerable.
5. If Captive Portal Basic Login is not enabled, the system is not vulnerable.



Indicators of Compromise

No evidence of compromise exists.

Mitigation

If you have NGFW 17.4.0, disable Captive Portal Basic Login.

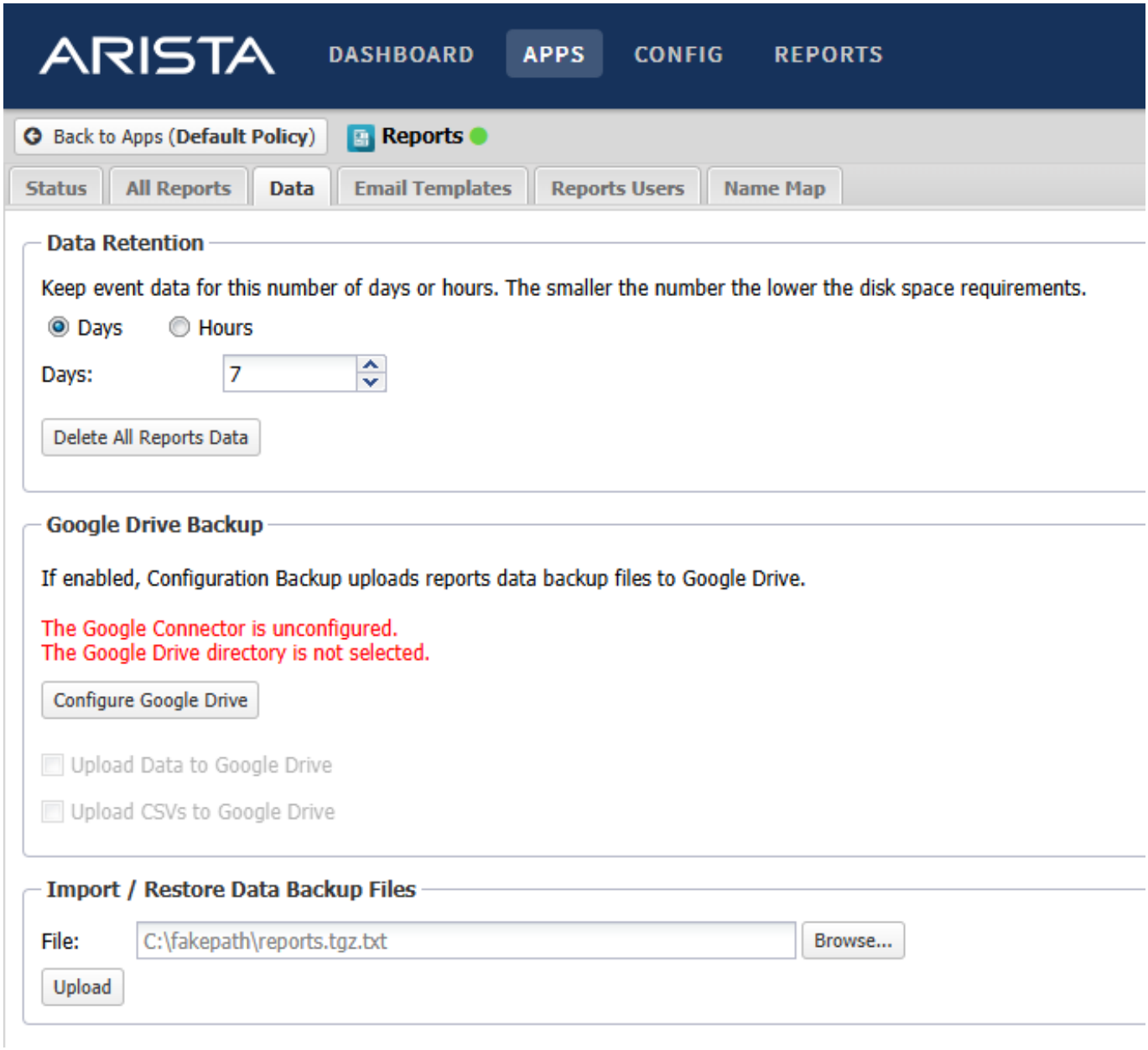
3) CVE-2026-25621 - Reports application vulnerability due to insecure input validation

Required Configuration for Exploitation

Verify the following;

1. An NGFW system, version 17.4.0. Earlier versions are not affected.

2. A successful attack requires administrative access to the NGFW UI.
3. As the NGFW administrator, log into the UI and navigate to the Reports application.
4. On the Data tab, for the Import/Restore Data Backup Files field, specify a specially crafted SQL file.



Indicators of Compromise

No evidence of compromise exists.

Mitigation

Per operational best practice security models, do not allow unauthorized administrative access to the administrative browser.

4) CVE-2026-25622 - Captive Portal Custom Handler command injection vulnerability

Required Configuration for Exploitation

A successful attack requires administrative access to the NGFW UI.

Indicators of Compromise

No evidence of compromise exists.

Mitigation

Per operational best practice security models, do not allow unauthorized administrative access to the administrative browser.

5) CVE-2026-25623 - Command execution vulnerability

Required Configuration for Exploitation

A successful attack requires administrative access to the NGFW UI.

Indicators of Compromise

No evidence of compromise exists.

Mitigation

Per operational best practice security models, do not allow unauthorized administrative access to the administrative browser.

6) CVE-2026-25624 - Administrative cross script vulnerability

Required Configuration for Exploitation

A successful attack requires administrative access to the NGFW UI.

Indicators of Compromise

No evidence of compromise exists.

Mitigation

Per operational best practice security models, do not allow unauthorized administrative access to the administrative browser.

Resolution

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

- Upgrade to NGFW Version 17.4.1

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