

Date: October 6, 2026

Revision	Date	Changes
1.0	October 6, 2026	Initial release

The CVE-ID tracking this issue: CVE-2026-102164
CVSSv3.1 Base Score: 3.1 (CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)
CVSSv4.0 Base Score: 2.3
(CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N)
Common Weakness Enumeration: [CWE-125](#): Out-of-bounds Read
This vulnerability is being tracked by BUG1774082.

Description

On affected Arista access points configured with VXLAN tunnelling and L2-proxy (a specific configuration unique to the VESPA use-case), a wireless client associated to the tunnelled SSID can send a crafted packet, causing the access point to reveal memory contents in network traffic. No write primitive or remote code execution is possible.

This issue was discovered internally by Arista, and the company is not aware of any malicious exploitation of this vulnerability in customer networks.

Vulnerability Assessment

Platform and Software Applicability Note

To determine actual exposure, operators should first check their software versions against the "Affected Software" list below. If your software release is not listed, your deployment is not vulnerable, regardless of the hardware platform in use.

Affected Software

Wi-Fi Access Point

- 22.0.1F-32 and below releases in the 22.x train
- 21.3.0M-13 and below releases in 21.x train
- All prior releases

Affected Platforms

The following products **are** affected by these vulnerabilities:

- Wi-Fi Access Points

The following products **are not** affected by these vulnerabilities:

- Arista EOS-based products:
 - 710 Series
 - 720D Series
 - 720XP/722XPM Series
 - 750X Series
 - 7010TX Series
 - 7020R/R4 Series
 - 7130 Series running EOS
 - 7170 Series
 - 7050X3/X4 Series
 - 7060X/X2/X4/X5/X6 Series
 - 7260X/X3 Series
 - 7280R/R2/R3/R4 Series
 - 7300X/X3 Series
 - 7320X Series
 - 7358X4 Series
 - 7368X4 Series
 - 7388X5 Series
 - 7500R/R2/R3 Series
 - 7800R3/R4 Series
 - 7700R4 Series
 - AWE 5000 Series
 - AWE 7200R Series
 - ZTX-7200 Series
 - CloudEOS
 - cEOS-lab
 - vEOS-lab
 - CloudVision eXchange, virtual or physical appliance
- CloudVision Portal on-premises, virtual appliance or physical appliance (including the CV-CUE on premises software)
- CloudVision CUE cloud service delivery
- CloudVision Appliance Software
- CloudVision as-a-Service
- CloudVision AGNI - Cloud service delivery
- CloudVision AGNI - Virtual or physical appliance
- Arista 7130 Systems running MOS
- Arista Converged Cloud Fabric (formerly Big Switch BCF)
- DANZ Monitoring Fabric (DMF) - Controller Appliance
- DANZ Monitoring Fabric (DMF) - Analytics Node Appliance
- DANZ Monitoring Fabric (DMF) - Recorder Node Appliance
- DANZ Monitoring Fabric (DMF) - Service Node Appliance
- Arista Multi Cloud Director (formerly Big Switch MCD)
- 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)

Required Configuration for Exploitation

VXLAN tunnelling with L2-proxy must be enabled. This is a non-default configuration. If L2-proxy is not configured, the access point is not exposed to this vulnerability. The issue can be triggered either from the LAN or by an associated client.

The screenshot shows the Arista configuration interface. On the left is a sidebar with navigation links: DASHBOARD, MONITOR, CONFIGURE (highlighted), TROUBLESHOOT, FLOOR PLAN, REPORTS, and SYSTEM. The main content area has tabs for 'Locations' and 'Nmap'. Below these is a 'Network Profiles' section with a 'Tunnel' button. The 'Tunnel Interface Name' configuration page is displayed. It includes a 'Tunnel Interface Name' field with a red asterisk and a 'Tunnel Type' dropdown menu set to 'VXLAN'. Below this, the 'L2 Proxy' checkbox is checked and circled in red. There are 'Primary' and 'Secondary' tabs, with 'Secondary' being the active tab. A message states: 'Secondary tunnel settings are disabled because L2 Proxy is enabled.' Below the tabs are three checkboxes: 'Enable Secondary Endpoint' (unchecked), 'Prefer Primary Endpoint' (checked), and 'Disconnect Clients On Switching End Points' (checked). At the bottom is a 'Remote Endpoint (Enter IP Address/Hostname)' field.

Indicators of Compromise

No indicators of compromise are available for this issue.

Mitigation

If VXLAN tunnelling with L2-proxy is not required, disabling this configuration eliminates exposure. Note: disabling L2-proxy will prevent DHCP proxying for wireless clients on VXLAN-

tunnelled SSIDs; affected clients will be unable to obtain IP addresses and will lose network connectivity on those SSIDs.

The screenshot shows the Arista Network Profiles configuration page for a Tunnel interface. The left sidebar contains navigation links: DASHBOARD, MONITOR, CONFIGURE (highlighted), TROUBLESHOOT, FLOOR PLAN, REPORTS, and SYSTEM. The main content area has tabs for 'Locations' and 'Nmap'. Below the 'Network Profiles' header, there is a 'Tunnel' button and a 'Tunnel Interface Name' section. The 'Tunnel Interface Name' field is labeled 'Tunnel Interface Name *' and contains the placeholder text 'Enter Tunnel Interface Name'. To the right, the 'Tunnel Type' dropdown menu is set to 'VXLAN'. Below these fields, there are two tabs: 'Primary' and 'Secondary' (highlighted). Under the 'Secondary' tab, there are three checkboxes: 'L2 Proxy' (highlighted with a red circle), 'Enable Secondary Endpoint', and 'Prefer Primary Endpoint'. Below these, there are two checked checkboxes: 'Disconnect Clients On Switching End Points' and 'Remote Endpoint (Enter IP Address/Hostname)'. The 'Remote Endpoint' field contains the placeholder text 'Enter IP Address/Hostname'.

Resolution

The recommended resolution is to upgrade to a remediated software version 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 [Schedule Access Point Update](#).

CVE-2026-102164 has been fixed in the following releases:

- 22.1.1F-61 and later release in the 22.x train
- 21.4.0M-12 and later releases in the 21.x train

Hotfix

No hotfix is available for this issue.

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>