Date: October 6, 2026

Revision	Date	Changes
1.0	October 6, 2026	Initial release

Description

Two security vulnerabilities have been identified in Arista access point firmware affecting the Captive Portal feature. Both vulnerabilities allow an unauthenticated wireless client that is associated with a captive-portal-enabled SSID to crash the portal service with a single crafted HTTP request.

All of these issues were discovered internally by Arista, and the company is not aware of any malicious exploitation of this vulnerability in customer networks.

CVE-2026-102168

On affected Arista Wi-Fi access points with Captive Portal enabled, an unauthenticated wireless client connected to a Captive-Portal-enabled SSID can crash the portal service with a crafted HTTP request. This results in a temporary denial of service until the service automatically restarts. Remote code execution is not possible.

CVSSv3.1 Base Score: 6.5 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CVSSv4.0 Base Score: 7.1
(CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-191: Integer Underflow (Wrap or Wraparound)
This vulnerability is being tracked by BUG 1774072

CVE-2026-102169

On affected Arista Wi-Fi access points with Captive Portal enabled, an unauthenticated wireless client connected to a captive-portal-enabled SSID can crash the portal service with a crafted HTTP request. The service automatically restarts, but a sustained low-rate attack can cause a persistent denial of service of the captive portal. Remote code execution is not possible.

CVSSv3.1 Base Score: 6.5 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CVSSv4.0 Base Score: 7.1
(CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-476: NULL Pointer Dereference
This vulnerability is being tracked by BUG 1846913

Vulnerability Assessment

Platform and Software Applicability Note

Copyright 2026 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.

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 the 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

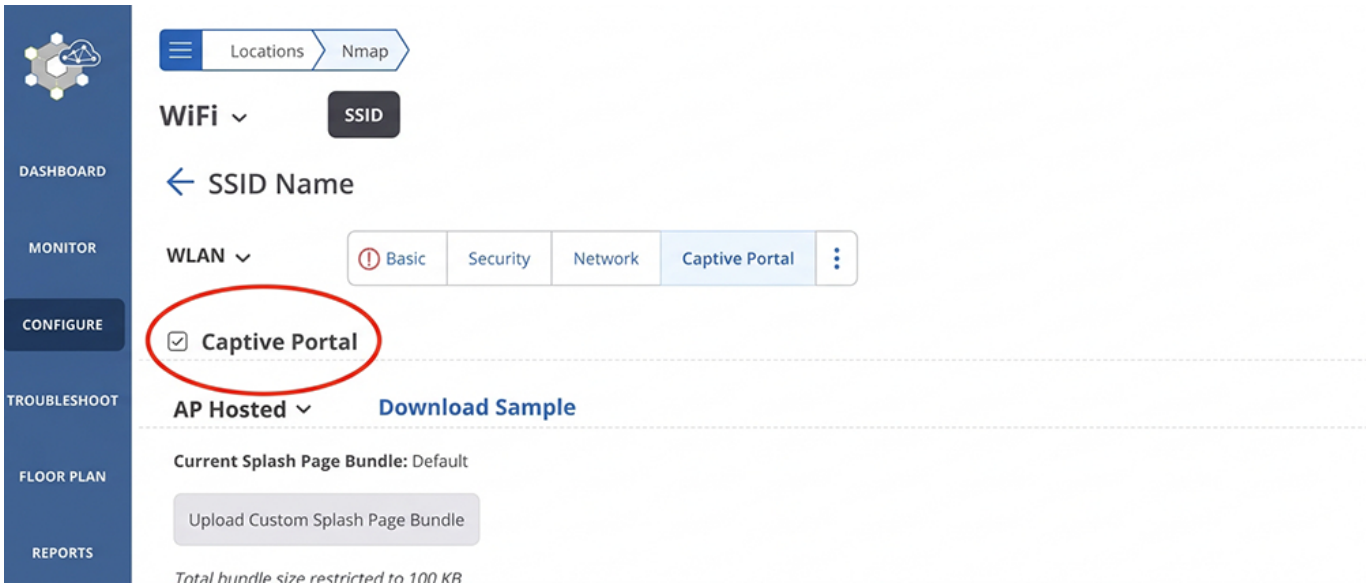
Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

    - 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

In order to be vulnerable to CVE-2026-102168 and CVE-2026-102169, Captive Portal must be enabled on at least one SSID, along with an associated client and LAN network. If the Captive Portal is not configured, the portal service is not running and the access point is not exposed to these vulnerabilities.

Copyright 2026 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.

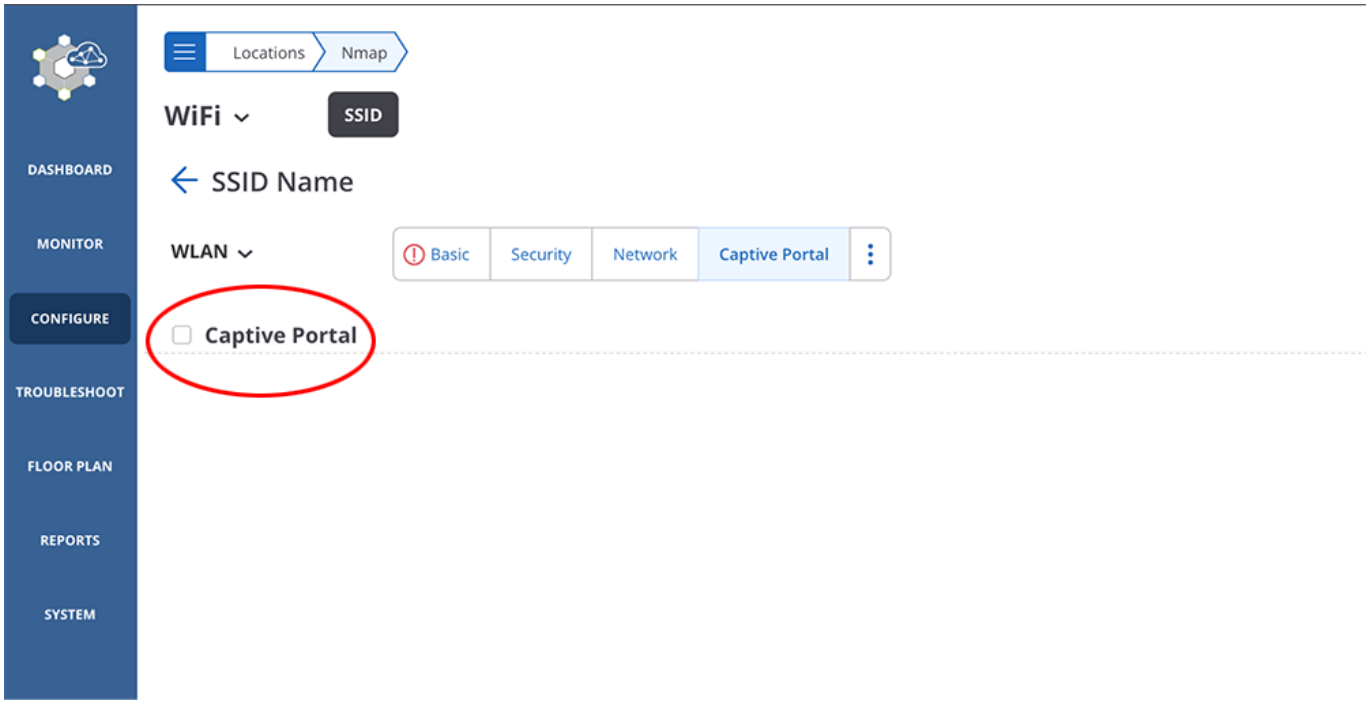


Indicators of Compromise

No indicators of compromise are available for this issue.

Mitigation

If Captive Portal is not required, disabling Captive Portal on all SSIDs eliminates exposure. If a Captive Portal is required, there is no mitigation available.



Resolution

Copyright 2026 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.

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-2026-102168 and CVE-2026-102169 have been fixed in the following releases:

- 22.1.1F 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

Copyright 2026 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.