September 29, 2026

Revision	Date	Changes
1.0	September 29, 2026	Initial release
1.1	October 6, 2026	Updated information

Update Type:

Informational

Background

Recent enhancements to our vulnerability detection processes have resulted in a higher-than-usual volume of security updates. Arista is providing this advance notification to help our customers plan. To streamline remediation efforts and allow customers to address them in a consolidated maintenance window, Arista is consolidating a larger volume of discrete advisories into aggregated bulk advisory releases. For more information about Arista's Vulnerability Management process, see: Device Hardening and Vulnerability Management.

Scope of the Upcoming Release

On October 6, 2026 Arista published multiple Security Advisories. This update serves as a summary of those security advisories. Customers are encouraged to review each advisory that may impact their environment to assess the vulnerability conditions as well as mitigation and remediation options.

Products Included in these Advisories:

- CloudVision Portal on-premises (referred to as "CVP" below)
- CV-CUE on-premises (referred to as "CV-CUE" below)
- Wi-Fi Access Point software

Note: The cloud service delivery of CloudVision Portal (aka CVaaS) and CloudVision CUE (CV-CUE) have already been remediated

Security Advisory #	Product (Component)	CVE ID	Severity	CVSS 3.1 Score
185	CVP (Fileserver)	CVE-2026-101158	High	8.4
186	CVP (OIDC SSO)	CVE-2026-101149 CVE-2026-101150	Medium	4.1

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.

187	CVP (Login)	CVE-2026-101151 CVE-2026-101152	High	8.0
188	CVP or CloudVision Sensor	CVE-2026-101153	High	8.0
189	CVP (Software Management Studio Repository Network Provisioning Image Repository)	CVE-2026-101154 CVE-2026-101155	Critical	9.1
190	CV-CUE	CVE-2026-102155 CVE-2026-102157 CVE-2026-102158 CVE-2026-102159 CVE-2026-102160 CVE-2026-102161	Critical	9.8
191	CV-CUE (LDAP Authentication)	CVE-2026-102156	Medium	6.8
192	CV-CUE (Network Config/ WIPS UI)	CVE-2026-101156 CVE-2026-101157	High	8.7
193	Wi-Fi AP (Captive Portal and Application Firewall)	CVE-2026-102162	High	8.8
194	Wi-Fi AP (Captive Portal)	CVE-2026-102168 CVE-2026-102169	Medium	6.5

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.

195	Wi-Fi AP (WIPS)	CVE-2026-102163	High	8.8
196	Wi-Fi AP (L2 Proxy)	CVE-2026-102164	Low	3.1
197	Wi-Fi AP (Sensor Service)	CVE-2026-102167	High	7.5
198	Wi-Fi AP (Live Packet Capture)	CVE-2026-102165	High	7.5

For More Information

If you have any general questions regarding this upcoming release process, please reach out to Arista TAC or your standard support contacts.

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.