

September 2, 2026

Revision	Date	Changes
1.0	September 02, 2026	Initial release
1.1	September 09, 2026	Updated Information

Update Type:

Informational

Scope of this Advisory:

On September 09, 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:

- Arista EOS
- VeloCloud

Security Advisory #	Product (Component)	CVE ID	Severity	CVSS 3.1 Score
149	EOS (802.1X)	CVE-2026-7344 9	Medium	5.9
150	EOS (802.1X)	CVE-2026-7719 1 CVE-2026-7594 3 CVE-2026-7594 4 CVE-2026-7594 5	Medium	4.5
151	EOS (ACL)	CVE-2026-7345 1	Medium	4.8
152	EOS (AuthN)	CVE-2026-1964 1	Medium	5.3
153	EOS (AuthN, TACACS)	CVE-2026-7346 5 CVE-2026-7346	Medium	6.3

Security Advisory #	Product (Component)	CVE ID	Severity	CVSS 3.1 Score
		6 CVE-2026-7346 7		
154	EOS (BFD)	CVE-2026-7345 8	High	8.2
155	EOS (DHCP Relay)	CVE-2026-1965 5	Medium	6.5
156	EOS (DHCP Relay)	CVE-2026-7343 7	Critical	9.6
157	EOS (FHRP / VRRP)	CVE-2026-7344 2 CVE-2026-7344 3 CVE-2026-7344 4	Medium	4.7
158	EOS (OpenConfig)	CVE-2026-7345 6 CVE-2026-7345 7	Critical	10
159	EOS (IGMP)	CVE-2026-7346 2	Medium	6.5
160	EOS (IS-IS)	CVE-2026-7344 6 CVE-2026-7345 9 CVE-2026-7346 0	High	7.4
161	EOS (MLAG)	CVE-2026-7345 0	Medium	6.9
162	EOS (OpenConfig)	CVE-2026-7344 7	Critical	9.1
163	EOS (OpenConfig)	CVE-2026-7346 1	High	8
164	EOS (OpenConfig)	CVE-2026-7343 9	High	7.5
165	EOS	CVE-2026-7345	High	8.1

Security Advisory #	Product (Component)	CVE ID	Severity	CVSS 3.1 Score
	(OpenConfig)	4		
166	EOS (OpenConfig)	CVE-2026-73464	High	8.8
167	EOS (OpenConfig)	CVE-2026-73445	Medium	4.9
168	EOS (OpenConfig)	CVE-2026-2380	High	7.4
169	EOS (OpenConfig)	CVE-2026-73463	Medium	5.3
170	EOS (OpenConfig)	CVE-2026-19640	Medium	4.2
171	EOS (OSPF)	CVE-2026-73435 CVE-2026-73436	High	8.2
172	EOS (OSPFv3)	CVE-2026-73438	Medium	5.3
173	EOS (OSPFv3)	CVE-2026-73455	High	7.5
174	EOS (P4Runtime)	CVE-2026-73453	Critical	10
175	EOS (PIM)	CVE-2026-73468	Medium	6.5
176	EOS (uRPF)	CVE-2026-73469	Medium	5.8
177	EOS (S4Sync)	CVE-2026-77190	Medium	6.5
178	EOS (SNMPv3)	CVE-2026-73440	Medium	4.2
179	VeloCloud Edge (HA)	CVE-2026-86106	Critical	9.6
180	VeloCloud Edge VeloCloud	CVE-2026-86107	Medium	5.9

Security Advisory #	Product (Component)	CVE ID	Severity	CVSS 3.1 Score
	Gateway (VCMP)			
181	VeloCloud Edge (Remote Diag)	CVE-2026-86108	High	8.0
182	VeloCloud Edge (Software Install)	CVE-2026-86109	Medium	6.6

Background

To assist our customers in planning for security updates, Arista previously issued an advance notification of this advisory regarding an increased volume of advisories resulting from recent improvements to our vulnerability detection processes. We are combining multiple discrete advisories into aggregated bulk releases to help consolidate maintenance windows and simplify remediation. For more information about Arista's Vulnerability Management process, see [Device Hardening and Vulnerability Management](#).

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.