



# CVE-2020-11622

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2020-11622
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-06-10 20:15:00 UTC
<b>Updated</b>	2020-06-23 19:24:00 UTC
<b>Description</b>	A vulnerability exists in Arista's Cloud EOS VM / vEOS 4.23.2M and below releases in the 4.23.x train, 4.22.4M and below

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Arista	Cloudeos	4.21.3fx-7368	All	All	All
Application	Arista	Cloudeos	4.21.4-fcrfx	All	All	All
Application	Arista	Cloudeos	4.21.4.1	All	All	All
Application	Arista	Cloudeos	4.21.7.1	All	All	All
Application	Arista	Cloudeos	4.22.2.0.1	All	All	All
Application	Arista	Cloudeos	4.22.2.2.1	All	All	All
Application	Arista	Cloudeos	4.22.3.1	All	All	All
Application	Arista	Cloudeos	4.23.2.1	All	All	All
Application	Arista	Cloudeos	4.21.3fx-7368	All	All	All
Application	Arista	Cloudeos	4.21.4-fcrfx	All	All	All
Application	Arista	Cloudeos	4.21.4.1	All	All	All
Application	Arista	Cloudeos	4.21.7.1	All	All	All
Application	Arista	Cloudeos	4.22.2.0.1	All	All	All
Application	Arista	Cloudeos	4.22.2.2.1	All	All	All
Application	Arista	Cloudeos	4.22.3.1	All	All	All
Application	Arista	Cloudeos	4.23.2.1	All	All	All
Application	Arista	Cloudeos	All	All	All	All

Application	<a href="#">Arista</a>	<a href="#">Cloudeos</a>	All	All	All	All
Application	<a href="#">Arista</a>	<a href="#">Cloudeos</a>	All	All	All	All
Application	<a href="#">Arista</a>	<a href="#">Veos</a>	4.21.3fx-7368	All	All	All
Application	<a href="#">Arista</a>	<a href="#">Veos</a>	4.21.4-fcrfx	All	All	All
Application	<a href="#">Arista</a>	<a href="#">Veos</a>	4.21.4.1	All	All	All
Application	<a href="#">Arista</a>	<a href="#">Veos</a>	4.21.7.1	All	All	All
Application	<a href="#">Arista</a>	<a href="#">Veos</a>	4.22.2.0.1	All	All	All
Application	<a href="#">Arista</a>	<a href="#">Veos</a>	4.22.2.2.1	All	All	All
Application	<a href="#">Arista</a>	<a href="#">Veos</a>	4.22.3.1	All	All	All
Application	<a href="#">Arista</a>	<a href="#">Veos</a>	4.23.2.1	All	All	All
Application	<a href="#">Arista</a>	<a href="#">Veos</a>	4.21.3fx-7368	All	All	All
Application	<a href="#">Arista</a>	<a href="#">Veos</a>	4.21.4-fcrfx	All	All	All
Application	<a href="#">Arista</a>	<a href="#">Veos</a>	4.21.4.1	All	All	All
Application	<a href="#">Arista</a>	<a href="#">Veos</a>	4.21.7.1	All	All	All
Application	<a href="#">Arista</a>	<a href="#">Veos</a>	4.22.2.0.1	All	All	All
Application	<a href="#">Arista</a>	<a href="#">Veos</a>	4.22.2.2.1	All	All	All
Application	<a href="#">Arista</a>	<a href="#">Veos</a>	4.22.3.1	All	All	All
Application	<a href="#">Arista</a>	<a href="#">Veos</a>	4.23.2.1	All	All	All
Application	<a href="#">Arista</a>	<a href="#">Veos</a>	All	All	All	All
Application	<a href="#">Arista</a>	<a href="#">Veos</a>	All	All	All	All
Application	<a href="#">Arista</a>	<a href="#">Veos</a>	All	All	All	All

## References

Reference	Source	Link	Tags
Security Advisory 0049 - Arista	CONFIRM	<a href="http://www.arista.com">www.arista.com</a>	Mitigation, Vendor Advisory
Advisories & Notices - Arista	MISC	<a href="http://www.arista.com">www.arista.com</a>	Vendor Advisory
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**