



# CVE-2020-3343

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

## Summary

<b>CVE</b>	CVE-2020-3343
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-05-22 06:15:00 UTC
<b>Updated</b>	2020-05-28 17:43:00 UTC
<b>Description</b>	A vulnerability in Cisco AMP for Endpoints Linux Connector Software and Cisco AMP for Endpoints Mac Connector Software

## Risk And Classification

**Problem Types:** CWE-120

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Advanced Malware Protection For Endpoints	All	All	All	All
Application	Cisco	Advanced Malware Protection For Endpoints	All	All	All	All

## References

Reference	Source	Link
Cisco AMP for Endpoints Linux Connector and AMP for Endpoints Mac Connector Software Memory Buffer Vulnerability	CISCO	<a href="#">tools.c</a>
CVE Program record	CVE.ORG	<a href="#">www.c</a>
NVD vulnerability detail	NVD	<a href="#">nvd.ni</a>

No vendor comments have been submitted for this CVE.

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

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](#)**