



CVE-2020-3335

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2020-3335
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-03 18:15:00 UTC
Updated	2021-08-06 18:40:00 UTC
Description	A vulnerability in the key store of Cisco Application Services Engine Software could allow an authenticated, local attacker to

Risk And Classification

Problem Types: CWE-863

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Application Policy Infrastructure Controller	1.1\(\0c\)	All	All	All
Application	Cisco	Application Policy Infrastructure Controller	1.1\(\0c\)	All	All	All
Application	Cisco	Application Services Engine	All	All	All	All
Application	Cisco	Application Services Engine	All	All	All	All

References

Reference	Source	Link	Tags
Cisco Application Services Engine Software Authorization Vulnerability	CISCO	tools.cisco.com	Patch, Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#)