



CVE-2016-1386

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

Summary

CVE	CVE-2016-1386
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-04-28 22:59:00 UTC
Updated	2016-12-03 03:20:00 UTC
Description	The API in Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) 1.0(1) allows remote attackers to

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Application Policy Infrastructure Controller Enterprise Module	1.0.(1)	All	All	All
Application	Cisco	Application Policy Infrastructure Controller Enterprise Module	1.0.\(1\)	All	All	All
Application	Cisco	Application Policy Infrastructure Controller Enterprise Module	1.0.\(1\)	All	All	All

References

Reference

- Cisco Application Policy Infrastructure Controller Enterprise Module Unauthorized Access Vulnerability
- Cisco Application Policy Infrastructure Controller Enterprise Module API Access Control Flaw Lets Remote Users Modify Data on the Target S
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](#).

Free CVE JSON API [cve.report/api](#)

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