



CVE-2016-6413

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

Summary

CVE	CVE-2016-6413
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-09-24 01:59:00 UTC
Updated	2017-07-30 01:29:00 UTC
Description	The installation procedure on Cisco Application Policy Infrastructure Controller (APIC) devices 1.3(2f) mishandles binary file

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	1.3(2f)	All	All	All
Application	Cisco	Application Policy Infrastructure Controller	1.3\2f)	All	All	All
Application	Cisco	Application Policy Infrastructure Controller	1.3\2f)	All	All	All

References

Reference	Source
Cisco Application Policy Infrastructure Controller Binary Privilege Escalation Vulnerability	CISCO
Cisco Application Policy Infrastructure Controller Installation Permissions Lets Local Users Obtain Root Privileges - SecurityTracker	SECTR
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

316938 Cisco Application Policy Infrastructure Controller Binary Privilege Escalation Vulnerability(cisco-sa-20160921-apic)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)