CVE-2017-3851

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-3851
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-22 19:59:00 UTC
Updated	2017-07-12 01:29:00 UTC
Description	A Directory Traversal vulnerability in the web framework code of the Cisco application-hosting framework (CAF) component

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Ios	1.1(0)	All	All	All
Application	Cisco	Ios	1.1.0	All	All	All
Application	Cisco	Ios	1.1\(0\)	All	All	All
Application	Cisco	Ios	1.1.0	All	All	All
Application	Cisco	Ios	1.1\(0\)	All	All	All

References

Reference
Cisco Application-Hosting Framework CVE-2017-3851 Directory Traversal Vulnerability
Cisco IOX for 800 Series Industrial Integrated Services Routers Input Validation Flaw Lets Remote Users Obtain Files on the Target System -
Cisco IOx for Cisco ASR 1000 Series Routers Input Validation Flaw Lets Remote Users Obtain Files on the Target System - SecurityTracker
Cisco Application-Hosting Framework Directory Traversal Vulnerability
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.

© 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 registred 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**