



CVE-2014-2147

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

Summary

CVE	CVE-2014-2147
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-02-12 01:59:00 UTC
Updated	2017-08-29 01:34:00 UTC
Description	The web interface in Cisco Prime Infrastructure 2.1 and earlier does not properly restrict use of IFRAME elements, which m

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Prime Infrastructure	All	All	All	All

References

Reference	Source
IBM X-Force Exchange	XF
Cisco Prime Infrastructure Web Interface Bugs Permit Cross-Site Scripting and Cross-Site Request Forgery Attacks - SecurityTracker	SECT
20150209 Cisco Prime Infrastructure Cross-Frame Scripting Vulnerability	CISCO
Cisco Prime Infrastructure CVE-2014-2147 Cross Frame Scripting Vulnerability	BID
tools.cisco.com/security/center/viewAlert.x	CONF
CVE Program record	CVE.C
NVD vulnerability detail	NVD

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 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](#)