



CVE-2017-6782

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

Summary

CVE	CVE-2017-6782
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-17 20:29:00 UTC
Updated	2017-08-25 10:51:00 UTC
Description	A vulnerability in the administrative web interface of Cisco Prime Infrastructure could allow an authenticated, remote attacker

Risk And Classification

Problem Types: CWE-94

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Prime Infrastructure	3.2(0.0)	All	All	All
Application	Cisco	Prime Infrastructure	3.2\0.0\	All	All	All
Application	Cisco	Prime Infrastructure	3.2\0.0\	All	All	All

References

Reference	Source	Li
Cisco Prime Infrastructure Flaw Lets Remote Users Inject HTML to Modify a Page on the Target System - SecurityTracker	SECTrack	w
Cisco Prime Infrastructure CVE-2017-6782 HTML Injection Vulnerability	BID	w
Cisco Prime Infrastructure HTML Injection Vulnerability	CISCO	to
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	ny

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](#)