



CVE-2013-5489

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2013-5489
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-09-13 14:10:00 UTC
Updated	2017-08-29 01:33:00 UTC
Description	The gadget implementation in Cisco SocialMiner does not properly restrict the content of GET requests, which allows remote attackers to bypass authentication and retrieve sensitive information.

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Socialminer	-	All	All	All
Application	Cisco	Socialminer	-	All	All	All

References

Reference	Source	Link	Tags
Cisco SocialMiner Sensitive Information GET Request Vulnerability	CISCO	tools.cisco.com	Vendor Advisory
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
Cisco SocialMiner Sensitive Information GET Request Vulnerability	CONFIRM	tools.cisco.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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](#).

CVE.report and Source URL Uptime Status status.cve.report