



CVE-2012-4615

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

Summary

CVE	CVE-2012-4615
State	PUBLIC
Assigner	security_alert@emc.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-11-27 21:55:00 UTC
Updated	2013-08-17 06:49:00 UTC
Description	EMC Smarts Network Configuration Manager (NCM) before 9.1 uses a hardcoded encryption key for the storage of credentials

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Emc	It Operations Intelligence	All	All	All	All

References

Reference	Source
EMC Smarts Network Configuration Manager (NCM) Multiple Security Bypass Vulnerabilities	BID
20121126 ESA-2012-057: EMC Smarts Network Configuration Manager Multiple Vulnerabilities	BUGTRAQ
EMC Smarts Network Configuration Manager Bypass ~ Packet Storm	MISC
EMC Smarts Network Configuration Manager Lets Local Users Gain Elevated Privileges - SecurityTracker	SECURITYTRACKER
87878	OSVDB
Security Advisory SA51408 - EMC Smarts Network Configuration Manager Database Authentication Bypass Vulnerability - Secunia	SECUNIA
CVE Program record	CVE.ORG
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](#)