



CVE-2012-4021

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

Summary

CVE	CVE-2012-4021
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-11-08 11:46:00 UTC
Updated	2013-03-02 04:44:00 UTC
Description	MosP kintai kanri before 4.1.0 does not properly perform authentication, which allows remote authenticated users to impersonate other users.

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mosp	Kintai Kanri	All	All	All	All

References

Reference	Source	Link	Tags
JVN#52264310: MosP kintai kanri vulnerable to authentication bypass	JVN	jvn.jp	
Security Advisory SA51110 - MosP Two Security Bypass Vulnerabilities - Secunia	SECUNIA	secunia.com	
JVNDB-2012-000097	JVNDB	jvndb.jvn.jp	
MosP CVE-2012-4021 Authentication Bypass Vulnerability	BID	www.securityfocus.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.

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