



CVE-2015-0532

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

Summary

CVE	CVE-2015-0532
State	PUBLIC
Assigner	security_alert@emc.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-05-01 10:59:00 UTC
Updated	2016-04-01 01:05:00 UTC
Description	EMC RSA Identity Management and Governance (IMG) 6.9 before P04 and 6.9.1 before P01 does not properly restrict pas

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Emc	Rsa Identity Management And Governance	6.9.0	All	All	All
Application	Emc	Rsa Identity Management And Governance	6.9.1	All	All	All
Application	Emc	Rsa Identity Management And Governance	6.9.0	All	All	All
Application	Emc	Rsa Identity Management And Governance	6.9.1	All	All	All

References

Reference	Source
RSA Identity Management and Governance Password Reset Weakness Lets Remote Users Gain Privileged Access - SecurityTracker	SECURITY
Bugtraq: ESA-2015-078: RSA® Identity Management and Governance (I MG) Insecure Password Reset Vulnerability	BUGTRAQ
RSA IMG 6.9 / 6.9.1 Insecure Password Reset ≈ Packet Storm	MISC
CVE Program record	CVE
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](#)