



CVE-2010-4274

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

Summary

CVE	CVE-2010-4274
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-11-17 01:00:00 UTC
Updated	2017-08-17 01:33:00 UTC
Description	reset_diragent_keys in the Common agent in IBM Systems Director 6.2.0 has 754 permissions, which allows local users to

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	Director Agent	6.2.0	All	All	All
Application	ibm	Director Agent	6.2.0	All	All	All

References

Reference

- IBM Systems Director Agent "reset_diragent_keys" Insecure File Permissions - Advisories - Community
- IBM X-Force Exchange
- SecurityTracker.com Archives - IBM Systems Director 'reset_diragent_keys' Unsafe File Permissions Lets Local Users Gain Elevated Privilege
- Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
- IBM Systems Director Agent 'reset_diragent_keys' Insecure File Permissions Vulnerability
- IBM IC71821: reset_diragent_keys has excessive file Permissions - United States
- CVE Program record
- NVD vulnerability detail

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)