



CVE-2009-2410

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

Summary

CVE	CVE-2009-2410
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-07-30 18:30:00 UTC
Updated	2017-08-17 01:30:00 UTC
Description	The local_handler_callback function in server/responder/pam/pam_LOCAL_domain.c in sssd 0.4.1 does not properly handle

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fedorahosted	Sssd	0.4.1	All	All	All
Application	Fedorahosted	Sssd	0.4.1	All	All	All

References

Reference

- [SECURITY] Fedora 11 Update: sssd-0.4.1-3.fc11
bugzilla.redhat.com/attachment.cgi
- 514057 – (CVE-2009-2410) CVE-2009-2410 If internal sssd user has no password set, the user can ssh to the sssd client with any supplied password
- Fedora SSSD BE Database No Password Authentication Bypass Vulnerability
- Fedora update for sssd - Secunia Advisories - Vulnerability Information - Secunia.com
- IBM X-Force Exchange
- 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](#)