



CVE-2018-10871

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

Summary

CVE	CVE-2018-10871
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-18 13:29:00 UTC
Updated	2019-10-09 23:33:00 UTC
Description	389-ds-base before versions 1.3.8.5, 1.4.0.12 is vulnerable to a Cleartext Storage of Sensitive Information. By default, when

Risk And Classification

Problem Types: CWE-312

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Fedoraproject	389 Directory Server	All	All	All	All
Application	Fedoraproject	389 Directory Server	All	All	All	All

References

Reference

- Issue #49789: By default, do not manage unhashed password - 389-ds-base - Pagure.io
- 1591480 – (CVE-2018-10871) CVE-2018-10871 389-ds-base: replication and the Retro Changelog plugin store plaintext password by default
- [SECURITY] [DLA 1483-1] 389-ds-base security update
- Red Hat Customer Portal
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

© [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](#)