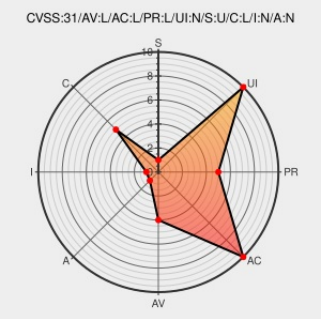
CVE-2010-3282

Published on: 01/09/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:03 PM UTC

CVE-2010-3282

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of 389 Directory Server from Fedoraproject contain the following vulnerability:

389 Directory Server before 1.2.7.1 (aka Red Hat Directory Server 8.2) and HP-UX Directory Server before B.08.10.03, when audit logging is enabled, logs the Directory Manager password (nsslapd-rootpw) in cleartext when changing cn=config:nsslapd-rootpw, which might allow local users to obtain sensitive information by reading the log.

CVE-2010-3282 has been assigned by hp-security-alert@hp.com to track the vulnerability - currently rated as LOW severity.

Affected Vendor/Software: **Red Hat** - **389 Directory Server** version **before 1.2.7.1**

Affected Vendor/Software: **HP** - **HP-UX Directory Server** version **before B.08.10.03**

CVSS3 Score: 3.3 - LOW

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	LOW	NONE	NONE

CVSS2 Score: 1.9 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link

625950 – (CVE-2010-3282) CVE-2010-3282 RHDS/389: information disclosure in audit logs	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=625950
OVAL - OVAL Repository	Not Applicable oval.mitre.org text/xml	OVAL oval:org.mitre.oval:def:6914
Document Display | HPE Support Center	Vendor Advisory support.hpe.com text/html	CONFIRM support.hpe.com/hpsc/doc/public/display?docId=emr_na-c02522633&docLocale=en_US
Infrastructure/Fedorahosted-retirement - Fedora Project Wiki	Product web.archive.org text/html Inactive Link Not Archived	CONFIRM git.fedorahosted.org/cgit/389/ds.git/commit/?id=d38ae06

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fedoraproject	389 Directory Server	All	All	All	All
Application	Fedoraproject	389 Directory Server	All	All	All	All
Application	Hp	Hp-ux Directory Server	All	All	All	All
Application	Hp	Hp-ux Directory Server	All	All	All	All
Application	Redhat	Directory Server	8.0	All	All	All
Application	Redhat	Directory Server	8.0	All	All	All
Application	Redhat	Redhat Directory Server	All	All	All	All
Application	Redhat	Redhat Directory Server	All	All	All	All

cpe:2.3:a:fedoraproject:389_directory_server:*:*:*:*:*:*:*:*:

cpe:2.3:a:fedoraproject:389_directory_server:*:*:*:*:*:*:*:*:

cpe:2.3:a:hp:hp-ux_directory_server:*:*:*:*:*:*:*:*:

cpe:2.3:a:hp:hp-ux_directory_server:*:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:directory_server:8.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:directory_server:8.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:redhat_directory_server:*:*:*:*:*:hp-ux:*:*:

cpe:2.3:a:redhat:redhat_directory_server:*:*:*:*:*:hp-ux:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 | |
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 registred 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