



CVE-2023-1055

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

Summary

CVE	CVE-2023-1055
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-02-27 22:15:00 UTC
Updated	2023-11-07 04:02:00 UTC
Description	A flaw was found in RHDS 11 and RHDS 12. While browsing entries LDAP tries to decode the userPassword attribute instea

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	36	All	All	All
Operating System	Fedoraproject	Fedora	37	All	All	All
Operating System	Fedoraproject	Fedora	38	All	All	All
Application	Redhat	Directory Server	11.5	All	All	All
Application	Redhat	Directory Server	11.6	All	All	All
Application	Redhat	Directory Server	12.0	All	All	All
Application	Redhat	Directory Server	12.1	All	All	All

References

Reference	Source
[SECURITY] Fedora 38 Update: 389-ds-base-2.3.5-1.fc38 - package-announce - Fedora Mailing-Lists	
[SECURITY] Fedora 38 Update: 389-ds-base-2.3.5-1.fc38 - package-announce - Fedora Mailing-Lists	FEDOR
2173517 – (CVE-2023-1055) CVE-2023-1055 RHDS: LDAP browser tries to decode userPassword instead of userCertificate attribute	MISC
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[284348](#) Fedora Security Update for 389 (FEDORA-2023-c92be0dfa0)

© [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](#)