



CVE-2021-3480

Published on: 05/20/2021 12:00:00 AM UTC

Last Modified on: 05/28/2021 07:58:00 PM UTC

CVE-2021-3480

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Fedora](#) from [Fedoraproject](#) contain the following vulnerability:

A flaw was found in slapi-nis in versions before 0.56.7. A NULL pointer dereference during the parsing of the Binding DN could allow an unauthenticated attacker to crash the 389-ds-base directory server. The highest threat from this vulnerability is to system availability.

CVE-2021-3480 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
[SECURITY] Fedora 34 Update: slapi-nis-0.56.7-1.fc34 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2021-f93243d461
[SECURITY] Fedora 33 Update: slapi-nis-0.56.7-1.fc33 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2021-a4ee3426c4

1944640 – (CVE-2021-3480) CVE-2021-3480 slapi-nis: NULL dereference (DoS) with specially crafted Binding DN

[bugzilla.redhat.com](https://bugzilla.redhat.com/text/html)
text/html

 MISC
bugzilla.redhat.com/show_bug.cgi?id=1944640

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.

Related QID Numbers

[159181](#) Oracle Enterprise Linux Security Update for slapi-nis (ELSA-2021-2032)

[159231](#) Oracle Enterprise Linux Security Update for idm:DL1 (ELSA-2021-1983)

[179758](#) Debian Security Update for slapi-nis (CVE-2021-3480)

[239278](#) Red Hat Update for slapi-nis (RHSA-2021:2032)

[239280](#) Red Hat Update for ipa (RHSA-2021:2027)

[239281](#) Red Hat Update for ipa (RHSA-2021:2026)

[239285](#) Red Hat Update for idm:DL1 (RHSA-2021:1983)

[281131](#) Fedora Security Update for slapi (FEDORA-2021-a4ee3426c4)

[281132](#) Fedora Security Update for slapi (FEDORA-2021-f93243d461)

[352382](#) Amazon Linux Security Advisory for slapi-nis: ALAS2-2021-1646

[376994](#) Alibaba Cloud Linux Security Update for slapi-nis (ALINUX2-SA-2021:0029)

[670590](#) EulerOS Security Update for slapi-nis (EulerOS-SA-2021-2348)

[670690](#) EulerOS Security Update for slapi-nis (EulerOS-SA-2021-2448)

[940415](#) AlmaLinux Security Update for idm:DL1 (ALSA-2021:1983)

[960006](#) Rocky Linux Security Update for idm:DL1 (RLSA-2021:1983)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Application	Slapi-nis Project	Slapi-nis	All	All	All	All
cpe:2.3:o:fedoraproject:fedora:33:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:34:*:*:*:*:*:						
cpe:2.3:a:slapi-nis_project:slapi-nis:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-3480 : A flaw was found in slapi-nis in versions before 0.56.7. A NULL pointer dereference during the pars... twitter.com/i/web/status/1...	2021-05-20 13:06:32
 /r/netcve	CVE-2021-3480	2021-05-20 13:41:45
← 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 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](#)