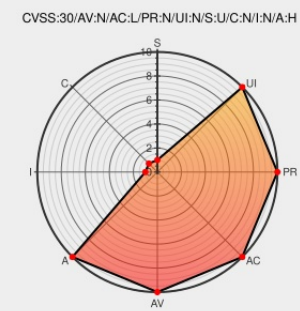
CVE-2018-14648

Published on: 09/28/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:43 PM UTC

CVE-2018-14648

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



Certain versions of Debian Linux from Debian contain the following vulnerability:

A flaw was found in 389 Directory Server. A specially crafted search query could lead to excessive CPU consumption in the do_search() function. An unauthenticated attacker could use this flaw to provoke a denial of service.

CVE-2018-14648 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **[UNKNOWN]** - **389-ds-base:** version **n/a**

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: 7.8 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
1630668 – (CVE-2018-14648) CVE-2018-14648 389-ds-base: Mishandled search requests in servers/slapd/search.c:do_search() allows for denial of service	Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-14648

Red Hat Customer Portal	Issue Tracking Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2018:3507
[SECURITY] [DLA 1554-1] 389-ds-base security update	Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20181025 [SECURITY] [DLA 1554-1] 389-ds-base security update
Red Hat Customer Portal - Access to 24x7 support and knowledge	Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2018:3127

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
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
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

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

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

cpe:2.3:o:redhat:enterprise_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:7.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report