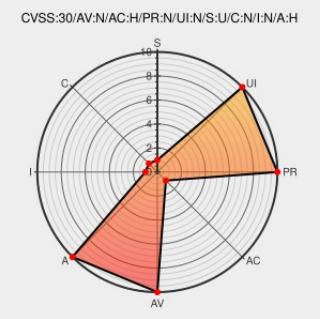
CVE-2018-10850

Published on: 06/13/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:22 PM UTC

CVE-2018-10850

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



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

389-ds-base before versions 1.4.0.10, 1.3.8.3 is vulnerable to a race condition in the way 389-ds-base handles persistent search, resulting in a crash if the server is under load. An anonymous attacker could use this flaw to trigger a denial of service.

CVE-2018-10850 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **[UNKNOWN]** - **389-ds-base** version **389-ds-base 1.4.0.10**

Affected Vendor/Software: **[UNKNOWN]** - **389-ds-base** version **389-ds-base 1.3.8.3**

CVSS3 Score: 5.9 - MEDIUM

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

CVSS2 Score: 7.1 - HIGH

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

CVE References

Description	Tags	Link

[SECURITY] [DLA 1428-1] 389-ds-base security update	Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20180715 [SECURITY] [DLA 1428-1] 389-ds-base security update
[security-announce] openSUSE-SU-2019:1397-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2019:1397
Issue #49768: Under network intensive load persistent search can erronously decrease connection refcnt - 389-ds-base - Pagure.io	Issue Tracking Third Party Advisory pagure.io text/html	CONFIRM pagure.io/389-ds-base/issue/49768
1588056 – (CVE-2018-10850) CVE-2018-10850 389-ds-base: race condition on reference counter leads to DoS using persistent search	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-10850
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2018:2757
Commit - 389-ds-base - 8f04487f99a - Pagure.io	Patch Third Party Advisory pagure.io text/html	CONFIRM pagure.io/389-ds-base/c/8f04487f99a

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
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All

Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	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:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.6:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.6:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_eus:7.5:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_eus:7.6:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_eus:7.5:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_eus:7.6:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_tus:7.6:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_tus:7.6:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:7.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→