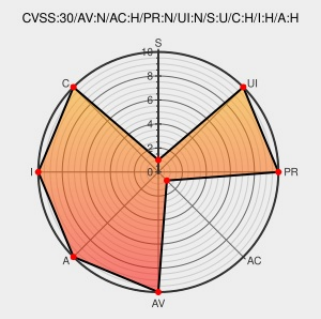
CVE-2017-8028

Published on: 11/27/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:42 PM UTC

CVE-2017-8028

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



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

In Pivotal Spring-LDAP versions 1.3.0 - 2.3.1, when connected to some LDAP servers, when no additional attributes are bound, and when using LDAP BindAuthenticator with org.springframework.ldap.core.support.DefaultTlsDirContextAuthenticationStrategy as the authentication strategy, and setting userSearch, authentication is allowed with an arbitrary password when the username is correct. This occurs because some LDAP vendors require an explicit operation for the LDAP bind to take effect.

CVE-2017-8028 has been assigned by secure@dell.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.1 - HIGH

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

CVSS2 Score: 5.1 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-4046-1 libspring-ldap-java	Issue Tracking Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-4046
CVE-2017-8028: Spring-LDAP authentication with userSearch and STARTTLS allows authentication with arbitrary password | Security | Pivotal	Issue Tracking Vendor Advisory pivotal.io text/html	CONFIRM pivotal.io/security/cve-2017-8028
[SECURITY] [DLA 1180-1] libspring-ldap-java security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20171119 [SECURITY] [DLA 1180-1] libspring-ldap-java security update
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2018:0319
Oracle Critical Patch Update Advisory - January 2021	www.oracle.com text/html	MISC www.oracle.com/security-alerts/cpujan2021.html

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	Pivotal Software	Spring-ldap	1.3.0	All	All	All
Application	Pivotal Software	Spring-ldap	1.3.1	All	All	All
Application	Pivotal Software	Spring-ldap	1.3.1	rc1	All	All
Application	Pivotal Software	Spring-ldap	1.3.2	All	All	All
Application	Pivotal Software	Spring-ldap	2.0.0	All	All	All
Application	Pivotal Software	Spring-ldap	2.0.1	All	All	All
Application	Pivotal Software	Spring-ldap	2.0.2	All	All	All
Application	Pivotal Software	Spring-ldap	2.0.3	All	All	All
Application	Pivotal Software	Spring-ldap	2.0.4	All	All	All
Application	Pivotal Software	Spring-ldap	2.1.0	All	All	All
Application	Pivotal Software	Spring-ldap	2.2.0	All	All	All
Application	Pivotal Software	Spring-ldap	2.2.1	All	All	All
Application	Pivotal Software	Spring-ldap	2.3.0	All	All	All

Application	Pivotal Software	Spring-ldap	2.3.1	All	All	All
Application	Pivotal Software	Spring-ldap	1.3.0	All	All	All
Application	Pivotal Software	Spring-ldap	1.3.1	All	All	All
Application	Pivotal Software	Spring-ldap	1.3.1	rc1	All	All
Application	Pivotal Software	Spring-ldap	1.3.2	All	All	All
Application	Pivotal Software	Spring-ldap	2.0.0	All	All	All
Application	Pivotal Software	Spring-ldap	2.0.1	All	All	All
Application	Pivotal Software	Spring-ldap	2.0.2	All	All	All
Application	Pivotal Software	Spring-ldap	2.0.3	All	All	All
Application	Pivotal Software	Spring-ldap	2.0.4	All	All	All
Application	Pivotal Software	Spring-ldap	2.1.0	All	All	All
Application	Pivotal Software	Spring-ldap	2.2.0	All	All	All
Application	Pivotal Software	Spring-ldap	2.2.1	All	All	All
Application	Pivotal Software	Spring-ldap	2.3.0	All	All	All
Application	Pivotal Software	Spring-ldap	2.3.1	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:pivotal_software:spring-ldap:1.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:pivotal_software:spring-ldap:1.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:pivotal_software:spring-ldap:1.3.1:rc1:*:*:*:*:*:*:

cpe:2.3:a:pivotal_software:spring-ldap:1.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:pivotal_software:spring-ldap:2.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:pivotal_software:spring-ldap:2.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:pivotal_software:spring-ldap:2.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:pivotal_software:spring-ldap:2.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:pivotal_software:spring-ldap:2.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:pivotal_software:spring-ldap:2.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:pivotal_software:spring-ldap:2.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:pivotal_software:spring-ldap:2.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:pivotal_software:spring-ldap:2.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:pivotal_software:spring-ldap:2.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:pivotal_software:spring-ldap:1.3.0:*:*:*:*:*:*:*

cpe:2.3:a:pivotal_software:spring-ldap:1.3.1:*:*:*:*:*:*:*

cpe:2.3:a:pivotal_software:spring-ldap:1.3.1:rc1:*:*:*:*:*:*

cpe:2.3:a:pivotal_software:spring-ldap:1.3.2:*:*:*:*:*:*:*

cpe:2.3:a:pivotal_software:spring-ldap:2.0.0:*:*:*:*:*:*:*

cpe:2.3:a:pivotal_software:spring-ldap:2.0.1:*:*:*:*:*:*:*

cpe:2.3:a:pivotal_software:spring-ldap:2.0.2:*:*:*:*:*:*:*

cpe:2.3:a:pivotal_software:spring-ldap:2.0.3:*:*:*:*:*:*:*

cpe:2.3:a:pivotal_software:spring-ldap:2.0.4:*:*:*:*:*:*:*

cpe:2.3:a:pivotal_software:spring-ldap:2.1.0:*:*:*:*:*:*:*

cpe:2.3:a:pivotal_software:spring-ldap:2.2.0:*:*:*:*:*:*:*

cpe:2.3:a:pivotal_software:spring-ldap:2.2.1:*:*:*:*:*:*:*

cpe:2.3:a:pivotal_software:spring-ldap:2.3.0:*:*:*:*:*:*:*

cpe:2.3:a:pivotal_software:spring-ldap:2.3.1:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→