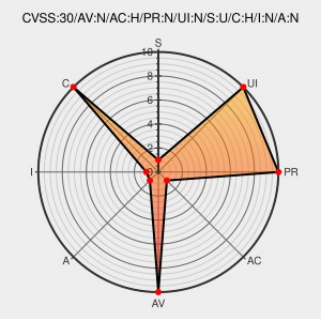
CVE-2014-3607

Published on: 01/08/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:46 PM UTC

CVE-2014-3607

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



Certain versions of Ldaptive from Ldaptive contain the following vulnerability:

DefaultHostnameVerifier in Ldaptive (formerly vt-ldap) does not properly verify that the server hostname matches a domain name in the subject's Common Name (CN) field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

CVE-2014-3607 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

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	HIGH	NONE	NONE

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
Google Code Archive - Long-term storage for Google Code Project Hosting.	Third Party Advisory code.google.com text/html	CONFIRM code.google.com/archive/p/vt-middleware/issues/228

1140438 – (CVE-2014-3607) CVE-2014-3607 vtldap/ldaptive: Hostname verification susceptible to MITM attack	Issue Tracking Patch Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1140438
	Third Party Advisory shibboleth.net text/plain	CONFIRM shibboleth.net/community/advisories/secadv_20140919.txt
Google Code Archive - Long-term storage for Google Code Project Hosting.	Third Party Advisory code.google.com text/html	CONFIRM code.google.com/archive/p/vt-middleware/issues/226
Google Code Archive - Long-term storage for Google Code Project Hosting.	Third Party Advisory code.google.com text/html	CONFIRM code.google.com/archive/p/vt-middleware/issues/227

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ldaptive	Ldaptive	All	All	All	All
Application	Ldaptive	Ldaptive	All	All	All	All
Application	Ldaptive	Vt-ldap	All	All	All	All
Application	Ldaptive	Vt-ldap	All	All	All	All

cpe:2.3:a:ldaptive:ldaptive:*:*:*:*:*:*:*:*:

cpe:2.3:a:ldaptive:ldaptive:*:*:*:*:*:*:*:*:

cpe:2.3:a:ldaptive:vt-ldap:*:*:*:*:*:*:*:*:

cpe:2.3:a:ldaptive:vt-ldap:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

site. This site includes MITRE data granted under the following license.

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