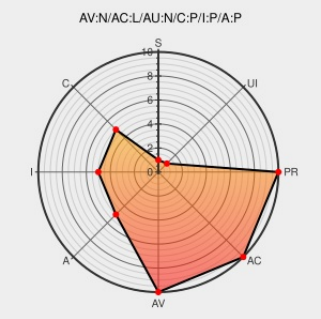
CVE-2006-0150

Published on: 01/09/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:07 PM UTC

CVE-2006-0150

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



Certain versions of Auth Ldap from Dave Carrigan contain the following vulnerability:

Multiple format string vulnerabilities in the auth_ldap_log_reason function in Apache auth_ldap 1.6.0 and earlier allows remote attackers to execute arbitrary code via various vectors, including the username.

CVE-2006-0150 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Apache auth_ldap module Multiple Format Strings Vulnerability - Digital Armaments for Intelligence	Vendor Advisory, www.digitalarmaments.com, text/html	MISC www.digitalarmaments.com/2006090173928420.html
Secunia - Advisories - Debian update for libapache-auth-ldap	Patch, Vendor Advisory, web.archive.org, text/html	SECUNIA 18568
Apache auth_ldap Module "auth_ldap_log_reason()" Format String Vulnerability - Advisories - Secunia	Patch, Vendor Advisory, web.archive.org, text/html	SECUNIA 18382
Advisories - Mandriva Linux	Patch, Vendor Advisory, www.new.mandriva.com	MANDRIVA MDKSA-2006:017

	text/html	
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20060109 Digital Armaments Security Advisory 01.09.2006: Apache auth_ldap module Multiple Format Strings Vulnerability
auth_ldap Format String Bug Lets Remote Users Execute Arbitrary Code - SecurityTracker	securitytracker.com text/html	SECTRACK 1015456
Red Hat update for auth_ldap - Advisories - Secunia	Patch Vendor Advisory web.archive.org text/html	SECUNIA 18405
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2006-0117
rhn.redhat.com | Red Hat Support	Patch Vendor Advisory www.redhat.com text/html	REDHAT RHSA-2006:0179
Mandriva update for mod_auth_ldap - Advisories - Secunia	Patch Vendor Advisory web.archive.org text/html	SECUNIA 18412
Debian -- Security Information -- DSA-952-1 libapache-auth-ldap	Patch Vendor Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-952
Dave Carrigan Auth_LDAP Remote Format String Vulnerability	Patch cve.report (archive) text/html	BID 16177
auth_ldap Change Log	web.archive.org text/html Inactive Link Not Archived	CONFIRM www.rudedog.org/auth_ldap/Changes.html
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF apache-authldap-format-string(24030)

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dave Carrigan	Auth Ldap	1.2.1	All	All	All
Application	Dave Carrigan	Auth Ldap	1.2.2	All	All	All
Application	Dave Carrigan	Auth Ldap	1.2.3	All	All	All
Application	Dave Carrigan	Auth Ldap	1.2.4	All	All	All

Application	Dave Carrigan	Auth Ldap	1.3.0	All	All	All
Application	Dave Carrigan	Auth Ldap	1.3.1	All	All	All
Application	Dave Carrigan	Auth Ldap	1.3.2	All	All	All
Application	Dave Carrigan	Auth Ldap	1.3.3	All	All	All
Application	Dave Carrigan	Auth Ldap	1.3.4	All	All	All
Application	Dave Carrigan	Auth Ldap	1.4.0	All	All	All
Application	Dave Carrigan	Auth Ldap	1.4.2	All	All	All
Application	Dave Carrigan	Auth Ldap	1.4.3	All	All	All
Application	Dave Carrigan	Auth Ldap	1.6.0	All	All	All
Application	Dave Carrigan	Auth Ldap	1.2.1	All	All	All
Application	Dave Carrigan	Auth Ldap	1.2.2	All	All	All
Application	Dave Carrigan	Auth Ldap	1.2.3	All	All	All
Application	Dave Carrigan	Auth Ldap	1.2.4	All	All	All
Application	Dave Carrigan	Auth Ldap	1.3.0	All	All	All
Application	Dave Carrigan	Auth Ldap	1.3.1	All	All	All
Application	Dave Carrigan	Auth Ldap	1.3.2	All	All	All
Application	Dave Carrigan	Auth Ldap	1.3.3	All	All	All
Application	Dave Carrigan	Auth Ldap	1.3.4	All	All	All
Application	Dave Carrigan	Auth Ldap	1.4.0	All	All	All
Application	Dave Carrigan	Auth Ldap	1.4.2	All	All	All
Application	Dave Carrigan	Auth Ldap	1.4.3	All	All	All
Application	Dave Carrigan	Auth Ldap	1.6.0	All	All	All

cpe:2.3:a:dave_carrigan:auth_ldap:1.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:dave_carrigan:auth_ldap:1.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:dave_carrigan:auth_ldap:1.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:dave_carrigan:auth_ldap:1.2.4:*:*:*:*:*:*:*:

cpe:2.3:a:dave_carrigan:auth_ldap:1.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:dave_carrigan:auth_ldap:1.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:dave_carrigan:auth_ldap:1.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:dave_carrigan:auth_ldap:1.3.3:*:*:*:*:*:*:*:

cpe:2.3:a:dave_carrigan:auth_ldap:1.3.4:*:*:*:*:*:*:*:

cpe:2.3:a:dave_carrigan:auth_ldap:1.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:dave_carrigan:auth_ldap:1.4.2:*:*:*:*:*:*:*:

cpe:2.3:a:dave_carrigan:auth_ldap:1.4.3:*:*:*:*:*:*:*:

cpe:2.3:a:dave_carrigan:auth_ldap:1.6.0:*:*:*:*:*:*:*:

cpe:2.3:a:dave_carrigan:auth_ldap:1.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:dave_carrigan:auth_ldap:1.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:dave_carrigan:auth_ldap:1.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:dave_carrigan:auth_ldap:1.2.4:*:*:*:*:*:*:*:

cpe:2.3:a:dave_carrigan:auth_ldap:1.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:dave_carrigan:auth_ldap:1.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:dave_carrigan:auth_ldap:1.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:dave_carrigan:auth_ldap:1.3.3:*:*:*:*:*:*:*:

cpe:2.3:a:dave_carrigan:auth_ldap:1.3.4:*:*:*:*:*:*:*:

cpe:2.3:a:dave_carrigan:auth_ldap:1.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:dave_carrigan:auth_ldap:1.4.2:*:*:*:*:*:*:*:

cpe:2.3:a:dave_carrigan:auth_ldap:1.4.3:*:*:*:*:*:*:*:

cpe:2.3:a:dave_carrigan:auth_ldap:1.6.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→