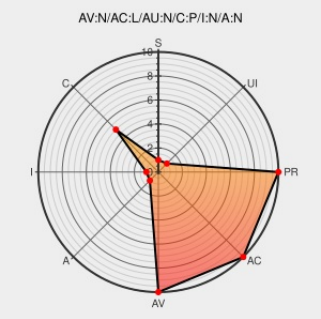
CVE-2005-3630

Published on: 12/31/2005 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:22 PM UTC

CVE-2005-3630

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



Certain versions of Fedora Core from Redhat contain the following vulnerability:

Fedora Directory Server before 10 allows remote attackers to obtain sensitive information, such as the password from adm.conf via an IFRAME element, probably involving an Apache httpd.conf configuration that orders "allow" directives before "deny" directives.

CVE-2005-3630 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Fedora Directory Server Password Information Disclosure Vulnerability	Patch, cve.report (archive), text/html	BID 16729
FDS10Announcement - Fedora Directory Server	web.archive.org, text/html, Inactive Link, Not Archived	CONFIRM directory.fedora.redhat.com/wiki/FDS10Announcement
	Patch, bugzilla.redhat.com, text/x-diff	MISC bugzilla.redhat.com/bugzilla/attachment.cgi?id=121994
Secunia - Advisories - Fedora Directory Server Admin Server Password Disclosure	Patch, Vendor Advisory, web.archive.org, text/html	SECUNIA 18939

174837 – CVE-2005-3630 use of IFRAME exposes password from adm.conf for users	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/bugzilla/show_bug.cgi?id=174837

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Redhat	Fedora Core	1.0	All	directory_server	All
Operating System	Redhat	Fedora Core	1.0	All	directory_server	All

cpe:2.3:o:redhat:fedora_core:1.0:*:directory_server:*:*:*:*:*:

cpe:2.3:o:redhat:fedora_core:1.0:*:directory_server:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→