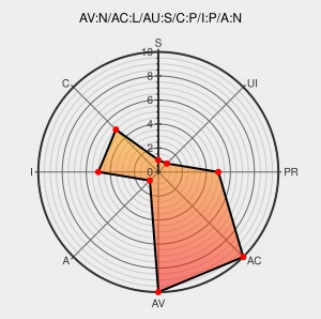
CVE-2012-1012

Published on: 06/07/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:17 PM UTC

CVE-2012-1012

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



Certain versions of Kerberos 5 from Mit contain the following vulnerability:

server/server_stubs.c in the kadmin protocol implementation in MIT Kerberos 5 (aka krb5) 1.10 before 1.10.1 does not properly restrict access to (1) SET_STRING and (2) GET_STRINGS operations, which might allow remote authenticated administrators to modify or read string attributes by leveraging the global list privilege.

CVE-2012-1012 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5.5 - MEDIUM

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

CVE References

Description	Tags	Link
796438 – (CVE-2012-1012) CVE-2012-1012 krb5: flaw in access control handling for strings in kadmin	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=796438
RT/krbdev.mit.edu: Ticket #7093 Access controls for string RPCs [CVE-2012-1012]	krbdev.mit.edu text/html	CONFIRM krbdev.mit.edu/rt/Ticket/Display.html?user=guest&pass=guest&id=7093
Kerberos 5 Release 1.10.3	web.mit.edu text/html	CONFIRM web.mit.edu/kerberos/krb5-1.10/
No Description Provided	src.mit.edu Inactive Link Not Archived	CONFIRM src.mit.edu/fisheye/changelog/krb5/?cs=25704

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mit	Kerberos 5	1.10	All	All	All
Application	Mit	Kerberos 5	1.10.1	All	All	All
Application	Mit	Kerberos 5	1.10	All	All	All
Application	Mit	Kerberos 5	1.10.1	All	All	All

cpe:2.3:a:mit:kerberos_5:1.10:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.10.1:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.10:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.10.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→