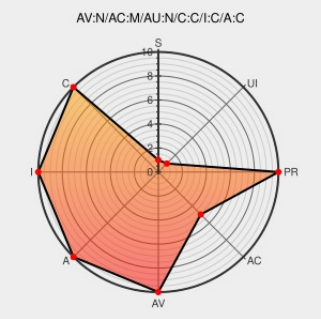
CVE-2012-1015

Published on: 08/06/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:19 PM UTC

CVE-2012-1015

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



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

The kdc_handle_protected_negotiation function in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) 1.8.x, 1.9.x before 1.9.5, and 1.10.x before 1.10.3 attempts to calculate a checksum before verifying that the key type is appropriate for a checksum, which allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized pointer free, heap memory corruption, and daemon crash) via a crafted AS-REQ request.

CVE-2012-1015 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 9.3 - HIGH

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

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-2518-1 krb5	www.debian.org Depreciated Link text/html	DEBIAN DSA-2518
openSUSE-SU-2012:0967-1: moderate: krb5: fixed several potential code ex	lists.opensuse.org text/html	SUSE openSUSE-SU-2012:0967
	Patch Vendor Advisory web.mit.edu text/x-diff	CONFIRM web.mit.edu/kerberos/advisories/MITKRB5-SA-2012-001.txt

Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2012:1131
Support / Security / Advisories / / MDVSA-2012:120 | Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2012:120

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	1.10.2	All	All	All
Application	Mit	Kerberos 5	1.8	All	All	All
Application	Mit	Kerberos 5	1.8.1	All	All	All
Application	Mit	Kerberos 5	1.8.2	All	All	All
Application	Mit	Kerberos 5	1.8.3	All	All	All
Application	Mit	Kerberos 5	1.8.4	All	All	All
Application	Mit	Kerberos 5	1.8.5	All	All	All
Application	Mit	Kerberos 5	1.8.6	All	All	All
Application	Mit	Kerberos 5	1.9.4	All	All	All
Application	Mit	Kerberos 5	1.10	All	All	All
Application	Mit	Kerberos 5	1.10.1	All	All	All
Application	Mit	Kerberos 5	1.10.2	All	All	All
Application	Mit	Kerberos 5	1.8	All	All	All
Application	Mit	Kerberos 5	1.8.1	All	All	All
Application	Mit	Kerberos 5	1.8.2	All	All	All
Application	Mit	Kerberos 5	1.8.3	All	All	All
Application	Mit	Kerberos 5	1.8.4	All	All	All
Application	Mit	Kerberos 5	1.8.5	All	All	All
Application	Mit	Kerberos 5	1.8.6	All	All	All
Application	Mit	Kerberos 5	1.9.4	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_5:1.10.2:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.8:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.8.1:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.8.2:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.8.3:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.8.4:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.8.5:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.8.6:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.9.4:*:*:*:*:*:*:*:

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_5:1.10.2:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.8:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.8.1:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.8.2:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.8.3:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.8.4:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.8.5:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.8.6:*:*:*:*:*:*:*:

cpe:2.3:a:mit:kerberos_5:1.9.4:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→