



CVE-2012-1016

Published on: 03/02/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:18 PM UTC

CVE-2012-1016

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Kerberos 5](#) from [Mit](#) contain the following vulnerability:

The `pkinit_server_return_padata` function in `plugins/preauth/pkinit/pkinit_srv.c` in the PKINIT implementation in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka `krb5`) before 1.10.4 attempts to find an agility KDF identifier in inappropriate circumstances, which allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a crafted Draft 9 request.

CVE-2012-1016 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
PKINIT (draft9) null ptr deref [CVE-2012-1016] · krb5/krb5@db64ca2 · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/krb5/krb5/commit/db64ca25d661a47b996b4e2645998b5d7f0eb52c
RT/krbdev.mit.edu: Ticket #7527 PKINIT (draft9) null ptr deref [CVE-2012-1016]	Vendor Advisory krbdev.mit.edu text/html	CONFIRM krbdev.mit.edu/rt/Ticket/Display.html?id=7527
Security Advisory SA55040 - Oracle Solaris Key Distribution Center (KDC) Denial of Service Vulnerabilities - Secunia	Third Party Advisory web.archive.org text/html	SECUNIA 55040

Kerberos 5 Release 1.10.6

[Release Notes](#)

[Vendor Advisory](#)

[web.mit.edu](#)

[text/html](#)



[CONFIRM web.mit.edu/kerberos/www/krb5-1.10/](https://web.mit.edu/kerberos/www/krb5-1.10/)

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	All	All	All	All
Application	Mit	Kerberos 5	All	All	All	All
cpe:2.3:a:mit:kerberos_5:*****:						
cpe:2.3:a:mit:kerberos_5:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)