



CVE-2015-8630

Published on: 02/12/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:13 PM UTC

CVE-2015-8630

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

The (1) `kadm5_create_principal_3` and (2) `kadm5_modify_principal` functions in `lib/kadm5/srv/svr_principal.c` in `kadmind` in MIT Kerberos 5 (aka `krb5`) 1.12.x and 1.13.x before 1.13.4 and 1.14.x before 1.14.1 allow remote authenticated users to cause a denial of service (NULL pointer dereference and daemon crash) by specifying

`KADM5_POLICY` with a NULL policy name.

CVE-2015-8630 has been assigned by [M](#) `cve@mitre.org` to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

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
Debian -- Security Information -- DSA-3466-1 krb5	www.debian.org Deprecated Link	DEBIAN DSA-3466

	text/html	
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2016:0532
Oracle Linux Bulletin - April 2016	www.oracle.com text/html	 CONFIRM www.oracle.com/technetwork/topics/security/linuxbulletinapr2016-2952096.html
Kerberos kadmind Policy Processing Null Pointer Dereference Lets Remote Authenticated Users Deny Service - SecurityTracker	www.securitytracker.com text/html	 SECTRACK 1034915
openSUSE-SU-2016:0406-1: moderate: Security update for krb5	lists.opensuse.org text/html	 SUSE openSUSE-SU-2016:0406
openSUSE-SU-2016:0501-1: moderate: Security update for krb5	lists.opensuse.org text/html	 SUSE openSUSE-SU-2016:0501
Check for null kadm5 policy name [CVE-2015-8630] · krb5/krb5@b863de7 · GitHub	Patch github.com text/html	 CONFIRM github.com/krb5/krb5/commit/b863de7fbf080b15e347a736fdda0a82d42f4f6b
#8342: Check for null kadm5 policy name [CVE-2015-8630]	krbdev.mit.edu text/html	 CONFIRM krbdev.mit.edu/rt/Ticket/Display.html?id=8342
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	1.12	All	All	All
Application	Mit	Kerberos 5	1.12.1	All	All	All
Application	Mit	Kerberos 5	1.12.2	All	All	All
Application	Mit	Kerberos 5	1.12.3	All	All	All
Application	Mit	Kerberos 5	1.12.4	All	All	All
Application	Mit	Kerberos 5	1.12.5	All	All	All
Application	Mit	Kerberos 5	1.13	All	All	All
Application	Mit	Kerberos 5	1.13.1	All	All	All
Application	Mit	Kerberos 5	1.13.2	All	All	All
Application	Mit	Kerberos 5	1.13.3	All	All	All
Application	Mit	Kerberos 5	1.14	All	All	All
Application	Mit	Kerberos 5	1.14	alpha1	All	All

Application	Mit	Kerberos 5	1.14	beta1	All	All
Application	Mit	Kerberos 5	1.14	beta2	All	All
Application	Mit	Kerberos 5	1.12	All	All	All
Application	Mit	Kerberos 5	1.12.1	All	All	All
Application	Mit	Kerberos 5	1.12.2	All	All	All
Application	Mit	Kerberos 5	1.12.3	All	All	All
Application	Mit	Kerberos 5	1.12.4	All	All	All
Application	Mit	Kerberos 5	1.12.5	All	All	All
Application	Mit	Kerberos 5	1.13	All	All	All
Application	Mit	Kerberos 5	1.13.1	All	All	All
Application	Mit	Kerberos 5	1.13.2	All	All	All
Application	Mit	Kerberos 5	1.13.3	All	All	All
Application	Mit	Kerberos 5	1.14	All	All	All
Application	Mit	Kerberos 5	1.14	alpha1	All	All
Application	Mit	Kerberos 5	1.14	beta1	All	All
Application	Mit	Kerberos 5	1.14	beta2	All	All
cpe:2.3:a:mit:kerberos_5:1.12:*:*:*:*:*:						
cpe:2.3:a:mit:kerberos_5:1.12.1:*:*:*:*:*:						
cpe:2.3:a:mit:kerberos_5:1.12.2:*:*:*:*:*:						
cpe:2.3:a:mit:kerberos_5:1.12.3:*:*:*:*:*:						
cpe:2.3:a:mit:kerberos_5:1.12.4:*:*:*:*:*:						
cpe:2.3:a:mit:kerberos_5:1.12.5:*:*:*:*:*:						
cpe:2.3:a:mit:kerberos_5:1.13:*:*:*:*:*:						
cpe:2.3:a:mit:kerberos_5:1.13.1:*:*:*:*:*:						
cpe:2.3:a:mit:kerberos_5:1.13.2:*:*:*:*:*:						
cpe:2.3:a:mit:kerberos_5:1.13.3:*:*:*:*:*:						
cpe:2.3:a:mit:kerberos_5:1.14:*:*:*:*:*:						
cpe:2.3:a:mit:kerberos_5:1.14:alpha1:*:*:*:*:						
cpe:2.3:a:mit:kerberos_5:1.14:beta1:*:*:*:*:						
cpe:2.3:a:mit:kerberos_5:1.14:beta2:*:*:*:*:						
cpe:2.3:a:mit:kerberos_5:1.12:*:*:*:*:*:						

cpe:2.3:a:mit:kerberos_5:1.12.1:*****:
cpe:2.3:a:mit:kerberos_5:1.12.2:*****:
cpe:2.3:a:mit:kerberos_5:1.12.3:*****:
cpe:2.3:a:mit:kerberos_5:1.12.4:*****:
cpe:2.3:a:mit:kerberos_5:1.12.5:*****:
cpe:2.3:a:mit:kerberos_5:1.13:*****:
cpe:2.3:a:mit:kerberos_5:1.13.1:*****:
cpe:2.3:a:mit:kerberos_5:1.13.2:*****:
cpe:2.3:a:mit:kerberos_5:1.13.3:*****:
cpe:2.3:a:mit:kerberos_5:1.14:*****:
cpe:2.3:a:mit:kerberos_5:1.14:alpha1:*****:
cpe:2.3:a:mit:kerberos_5:1.14:beta1:*****:
cpe:2.3:a:mit:kerberos_5:1.14:beta2:*****:

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](#)