

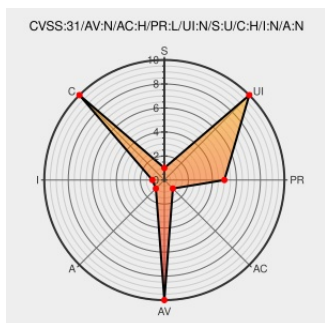


CVE-2015-8629

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

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

CVE-2015-8629

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

Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

The xdr_nullstring function in lib/kadm5/kadm_rpc_xdr.c in kadmind in MIT Kerberos 5 (aka krb5) before 1.13.4 and 1.14.x before 1.14.1 does not verify whether '\0' characters exist as expected, which allows remote authenticated users to obtain sensitive information or cause a denial of service (out-of-bounds read) via a crafted string.

CVE-2015-8629 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.3 - MEDIUM**

Attack
Vector

Attack
Complexity

Privileges
Required

User
Interaction

NETWORK

HIGH

LOW

NONE

Scope

Confidentiality
Impact

Integrity
Impact

Availability
Impact

UNCHANGED

HIGH

NONE

NONE

CVSS2 Score: **2.1 - LOW**

Access
Vector

Access
Complexity

Authentication

NETWORK

HIGH

SINGLE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

PARTIAL

NONE

NONE

CVE References

Description

Tags

Link

Oracle Solaris Bulletin - April 2016

[Third Party Advisory](#)
[www.oracle.com](#)
[text/html](#)

[CONFIRM](#) www.oracle.com/technetwork/topics/security/bulletinapr2016-2952098.html

Verify decoded kadmin C strings [CVE-2015-8629] · krb5/krb5@df17a12 · GitHub	Patch Third Party Advisory github.com text/html	 CONFIRM github.com/krb5/krb5/commit/df17a1224a3406f57477bcd372c61e04c0e5a5bb
Debian -- Security Information -- DSA-3466-1 krb5	Third Party Advisory www.debian.org Deprecated Link text/html	 DEBIAN DSA-3466
MIT Kerberos 5 CVE-2015-8629 Information Disclosure Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	 BID 82801
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2016:0532
Kerberos kadmind Null Termination Bug in xdr_nullstring() Lets Remote Authenticated Users Obtain Potentially Sensitive Information - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	 SECTrack 1034914
Oracle Linux Bulletin - April 2016	Third Party Advisory www.oracle.com text/html	 CONFIRM www.oracle.com/technetwork/topics/security/linuxbulletinapr2016-2952096.html
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2016:0493
openSUSE-SU-2016:0406-1: moderate: Security update for krb5	Mailing List Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2016:0406
openSUSE-SU-2016:0501-1: moderate: Security update for krb5	Mailing List Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2016:0501
#8341: Verify decoded kadmin C strings [CVE-2015-8629]	Vendor Advisory krbdev.mit.edu text/html	 CONFIRM krbdev.mit.edu/rt/Ticket/Display.html?id=8341

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
Operating System	Debian	Debian Linux	7.0	All	All	All

Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Mit	Kerberos 5	All	All	All	All
Application	Mit	Kerberos 5	All	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Oracle	Linux	6	-	All	All
Operating System	Oracle	Linux	7	-	All	All
Operating System	Oracle	Linux	6	-	All	All
Operating System	Oracle	Linux	7	-	All	All
Operating System	Oracle	Solaris	10	All	All	All
Operating System	Oracle	Solaris	11.3	All	All	All
Operating System	Oracle	Solaris	10	All	All	All
Operating System	Oracle	Solaris	11.3	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.7	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.2	All	All	All
Operating	Redhat	Enterprise Linux Eus	7.3	All	All	All

System						
Operating System	Redhat	Enterprise Linux Eus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.7	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.3	All	All	All
Operating	Redhat	Enterprise Linux Server Aus	7.4	All	All	All

System						
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:						
cpe:2.3:a:mit:kerberos_5:*:*:*:*:*:						
cpe:2.3:a:mit:kerberos_5:*:*:*:*:*:						
cpe:2.3:o:opensuse:leap:42.1:*:*:*:*:*:						
cpe:2.3:o:opensuse:leap:42.1:*:*:*:*:*:						
cpe:2.3:o:opensuse:opensuse:13.2:*:*:*:*:*:						
cpe:2.3:o:opensuse:opensuse:13.2:*:*:*:*:*:						

cpe:2.3:o:oracle:linux:6:-:*:*:*:*:*:
cpe:2.3:o:oracle:linux:7:-:*:*:*:*:*:
cpe:2.3:o:oracle:linux:6:-:*:*:*:*:*:
cpe:2.3:o:oracle:linux:7:-:*:*:*:*:*:
cpe:2.3:o:oracle:solaris:10:*:*:*:*:*:
cpe:2.3:o:oracle:solaris:11.3:*:*:*:*:*:
cpe:2.3:o:oracle:solaris:10:*:*:*:*:*:
cpe:2.3:o:oracle:solaris:11.3:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_desktop:6.0:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_desktop:6.0:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_eus:6.7:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_eus:7.2:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_eus:7.3:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_eus:7.4:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_eus:7.5:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_eus:7.6:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_eus:7.7:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_eus:6.7:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_eus:7.2:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_eus:7.3:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_eus:7.4:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_eus:7.5:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_eus:7.6:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_eus:7.7:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server:6.0:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server:7.0:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server:6.0:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:7.0:*****:

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.2:*****:

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.3:*****:

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.4:*****:

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.6:*****:

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.7:*****:

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.2:*****:

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.3:*****:

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.4:*****:

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.6:*****:

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.7:*****:

cpe:2.3:o:redhat:enterprise_linux_server_tus:7.2:*****:

cpe:2.3:o:redhat:enterprise_linux_server_tus:7.3:*****:

cpe:2.3:o:redhat:enterprise_linux_server_tus:7.6:*****:

cpe:2.3:o:redhat:enterprise_linux_server_tus:7.7:*****:

cpe:2.3:o:redhat:enterprise_linux_server_tus:7.2:*****:

cpe:2.3:o:redhat:enterprise_linux_server_tus:7.3:*****:

cpe:2.3:o:redhat:enterprise_linux_server_tus:7.6:*****:

cpe:2.3:o:redhat:enterprise_linux_server_tus:7.7:*****:

cpe:2.3:o:redhat:enterprise_linux_workstation:6.0:*****:

cpe:2.3:o:redhat:enterprise_linux_workstation:7.0:*****:

cpe:2.3:o:redhat:enterprise_linux_workstation:6.0:*****:

cpe:2.3:o:redhat:enterprise_linux_workstation:7.0:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)