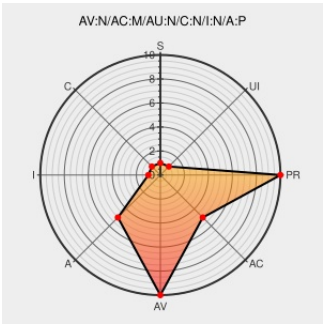
CVE-2010-0433

Published on: 03/05/2010 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:16:00 AM UTC

CVE-2010-0433

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



Certain versions of Openssl from Openssl contain the following vulnerability:

The kssl_keytab_is_available function in ssl/kssl.c in OpenSSL before 0.9.8n, when Kerberos is enabled but Kerberos configuration files cannot be opened, does not check a certain return value, which allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via SSL cipher negotiation, as demonstrated by a chroot installation of Dovecot or stunnel without Kerberos configuration files inside the chroot.

CVE-2010-0433 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
No Description Provided	kb.bluecoat.com Inactive Link Not Archived	CONFIRM kb.bluecoat.com/index?page=content&id=SA50
[syslog-ng-announce] syslog-ng Premium Edition 3.2.1a has been released	lists.balabit.com text/html	MLIST [syslog-ng-announce] 20110110 syslog-ng Premium Edition 3.2.1a has be
Webmail : Solution de messagerie professionnelle -	www.vupen.com text/html	VUPEN ADV-2010-0839

OVHcloud- OVH		
[SECURITY] Fedora 11 Update: openssl-0.9.8n-1.fc11	lists.fedoraproject.org text/html	FEDORA FEDORA-2010-5357
	aix.software.ibm.com text/plain	CONFIRM aix.software.ibm.com/aix/efixes/security/openssl_advisory.asc
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2010-0933
About Secunia Research | Flexera	secunia.com Depreciated Link text/plain	SECUNIA 42724
IBM AIX update for OpenSSL - Advisories - Community	web.archive.org text/html	SECUNIA 39932
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2010-1216
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20110211 VMSA-2011-0003 Third party component updates for VMw vCenter Update Manager, ESXi and ESX
[Dovecot] segfault - (imap|pop3)-login during nessus scan	www.mail-archive.com text/html	MLIST [dovecot] 20100219 segfault - (imap|pop3)-login during nessus scan
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:9856
Bug 567711 – Nessus PCI scan segfaults openssl dependent products due to kerberos enabled in openssl	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=567711
VMSA-2011-0003	www.vmware.com text/html	CONFIRM www.vmware.com/security/advisories/VMSA-2011-0003.html
Security Advisories | Mandriva Linux	www.mandriva.com text/html	MANDRIVA MDVSA-2010:076
About Secunia Research | Flexera	secunia.com Depreciated Link text/plain	SECUNIA 42733
'[security bulletin] HPSBUX02517 SSRT100058 rev.1 - HP-UX Running OpenSSL, Remote Unauthorized Inform' - MARC	marc.info text/html	HP HPSBUX02517
Fedora update for openssl - Advisories - Community	web.archive.org text/html	SECUNIA 39461
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:6718
Bug 569774 – CVE-2010-0433 openssl: crash	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=569774

caused by a missing krb5_sname_to_principal() return value check		
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:12260
[SECURITY] Fedora 13 Update: openssl-1.0.0-1.fc13	lists.fedoraproject.org text/html	FEDORA FEDORA-2010-5744
oss-security - OpenSSL (with KRB5) remote crash - CVE-2010-0433	www.openwall.com text/html	MLIST [oss-security] 20100303 OpenSSL (with KRB5) remote crash - CVE-2010
stunnel crashes with weak certificates... could it be OpenSSL? - mailing.openssl.users | Google Groups	groups.google.com text/html	MISC groups.google.com/group/mailing.openssl.users/browse_thread/thread/c3e1ab0034
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2010-0916
'[security bulletin] HPSBUX02531 SSRT100108 rev.1 - HP-UX Running Apache-based Web Server, Remote Den' - MARC	marc.info text/html	HP HPSBUX02531
[syslog-ng-announce] syslog-ng Premium Edition 3.0.6a has been released	lists.balabit.com text/html	MLIST [syslog-ng-announce] 20110110 syslog-ng Premium Edition 3.0.6a has be
VMware vCenter Server OpenSSL Denial of Service Vulnerabilities - Advisories - Community	web.archive.org text/html	SECUNIA 43311
VMware vCenter Server 4.1 Update 1 Release Notes	www.vmware.com text/html	CONFIRM www.vmware.com/support/vsphere4/doc/vsp_vc41_u1_rel_notes.htm
No Description Provided	cvs.openssl.org Inactive Link Not Archived	CONFIRM cvs.openssl.org/chngview?cn=19374
/news/changelog.html	www.openssl.org text/html	CONFIRM www.openssl.org/news/changelog.html

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	Openssl	Openssl	0.9.8	All	All	All
Application	Openssl	Openssl	0.9.8a	All	All	All
Application	Openssl	Openssl	0.9.8b	All	All	All
Application	Openssl	Openssl	0.9.8c	All	All	All
Application	Openssl	Openssl	0.9.8d	All	All	All
Application	Openssl	Openssl	0.9.8e	All	All	All
Application	Openssl	Openssl	0.9.8f	All	All	All
Application	Openssl	Openssl	0.9.8g	All	All	All
Application	Openssl	Openssl	0.9.8h	All	All	All
Application	Openssl	Openssl	0.9.8i	All	All	All
Application	Openssl	Openssl	0.9.8j	All	All	All
Application	Openssl	Openssl	0.9.8k	All	All	All
Application	Openssl	Openssl	0.9.8l	All	All	All
Application	Openssl	Openssl	All	All	All	All
Application	Openssl	Openssl	0.9.8	All	All	All
Application	Openssl	Openssl	0.9.8a	All	All	All
Application	Openssl	Openssl	0.9.8b	All	All	All
Application	Openssl	Openssl	0.9.8c	All	All	All
Application	Openssl	Openssl	0.9.8d	All	All	All
Application	Openssl	Openssl	0.9.8e	All	All	All
Application	Openssl	Openssl	0.9.8f	All	All	All
Application	Openssl	Openssl	0.9.8g	All	All	All
Application	Openssl	Openssl	0.9.8h	All	All	All
Application	Openssl	Openssl	0.9.8i	All	All	All
Application	Openssl	Openssl	0.9.8j	All	All	All
Application	Openssl	Openssl	0.9.8k	All	All	All
Application	Openssl	Openssl	0.9.8l	All	All	All

cpe:2.3:a:openssl:openssl:0.9.8:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8a:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8b:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8c:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8d:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8e:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8f:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8g:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8h:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8i:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8j:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8k:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8l:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:*:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8a:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8b:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8c:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8d:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8e:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8f:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8g:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8h:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8i:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8j:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8k:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8l:*:*:*:*:*:*:*:

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 registred 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