CVE-2014-3567

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2014-3567
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-10-19 01:55:00 UTC
Updated	2023-11-07 02:20:00 UTC
Description	Memory leak in the tls_decrypt_ticket function in t1_lib.c in OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1

Risk And Classification

Problem Types: CWE-20 | CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openssl	Openssl	1.0.0	All	All	All
Application	Openssl	Openssl	1.0.0	beta1	All	All
Application	Openssl	Openssl	1.0.0	beta2	All	All
Application	Openssl	Openssl	1.0.0	beta3	All	All
Application	Openssl	Openssl	1.0.0	beta4	All	All
Application	Openssl	Openssl	1.0.0	beta5	All	All
Application	Openssl	Openssl	1.0.0a	All	All	All
Application	Openssl	Openssl	1.0.0b	All	All	All
Application	Openssl	Openssl	1.0.0c	All	All	All
Application	Openssl	Openssl	1.0.0d	All	All	All
Application	Openssl	Openssl	1.0.0e	All	All	All
Application	Openssl	Openssl	1.0.0f	All	All	All
Application	Openssl	Openssl	1.0.0g	All	All	All
Application	Openssl	Openssl	1.0.0h	All	All	All
Application	Openssl	Openssl	1.0.0i	All	All	All
Application	Openssl	Openssl	1.0.0j	All	All	All
Application	Openssl	Openssl	1.0.0k	All	All	All

Application	Openssl	Openssl	1.0.0l	All	All	All
Application	Openssl	Openssl	1.0.0m	All	All	All
Application	Openssl	Openssl	1.0.0n	All	All	All
Application	Openssl	Openssl	1.0.1	All	All	All
Application	Openssl	Openssl	1.0.1	beta1	All	All
Application	Openssl	Openssl	1.0.1	beta2	All	All
Application	Openssl	Openssl	1.0.1	beta3	All	All
Application	Openssl	Openssl	1.0.1a	All	All	All
Application	Openssl	Openssl	1.0.1b	All	All	All
Application	Openssl	Openssl	1.0.1c	All	All	All
Application	Openssl	Openssl	1.0.1d	All	All	All
Application	Openssl	Openssl	1.0.1e	All	All	All
Application	Openssl	Openssl	1.0.1f	All	All	All
Application	Openssl	Openssl	1.0.1g	All	All	All
Application	Openssl	Openssl	1.0.1h	All	All	All
Application	Openssl	Openssl	1.0.1i	All	All	All
Application	Openssl	Openssl	All	All	All	All
Application	Openssl	Openssl	1.0.0	All	All	All
Application	Openssl	Openssl	1.0.0	beta1	All	All
Application	Openssl	Openssl	1.0.0	beta2	All	All
Application	Openssl	Openssl	1.0.0	beta3	All	All
Application	Openssl	Openssl	1.0.0	beta4	All	All
Application	Openssl	Openssl	1.0.0	beta5	All	All
Application	Openssl	Openssl	1.0.0a	All	All	All
Application	Openssl	Openssl	1.0.0b	All	All	All
Application	Openssl	Openssl	1.0.0c	All	All	All
Application	Openssl	Openssl	1.0.0d	All	All	All
Application	Openssl	Openssl	1.0.0e	All	All	All
Application	Openssl	Openssl	1.0.0f	All	All	All
Application	Openssl	Openssl	1.0.0g	All	All	All
Application	Openssl	Openssl	1.0.0h	All	All	All
Application	Openssl	Openssl	1.0.0i	All	All	All
Application	Openssl	Openssl	1.0.0j	All	All	All
Application	Openssl	Openssl	1.0.0k	All	All	All
Application	Openssl	Openssl	1.0.0l	All	All	All

Application	Openssl	Openssl	1.0.0m	All	All	All
Application	Openssl	Openssl	1.0.0n	All	All	All
Application	Openssl	Openssl	1.0.1	All	All	All
Application	Openssl	Openssl	1.0.1	beta1	All	All
Application	Openssl	Openssl	1.0.1	beta2	All	All
Application	Openssl	Openssl	1.0.1	beta3	All	All
Application	Openssl	Openssl	1.0.1a	All	All	All
Application	Openssl	Openssl	1.0.1b	All	All	All
Application	Openssl	Openssl	1.0.1c	All	All	All
Application	Openssl	Openssl	1.0.1d	All	All	All
Application	Openssl	Openssl	1.0.1e	All	All	All
Application	Openssl	Openssl	1.0.1f	All	All	All
Application	Openssl	Openssl	1.0.1g	All	All	All
Application	Openssl	Openssl	1.0.1h	All	All	All
Application	Openssl	Openssl	1.0.1i	All	All	All

References

Reference	Source	L
Red Hat Customer Portal	REDHAT	rh
McAfee KnowledgeBase - McAfee Security Bulletin - Three SSLv3 Vulnerabilities	CONFIRM	k
'[security bulletin] HPSBMU03267 rev.1 - HP Matrix Operating Environment and HP CloudSystem Matrix ru' - MARC	HP	m
'[security bulletin] HPSBMU03263 rev.3 - HP Insight Control running OpenSSL, Remote Disclosure of Inf' - MARC	HP	m
Mageia Advisory: MGASA-2014-0416 - Updated openssl packages fix security vulnerabilities	CONFIRM	a
Support / Security / Advisories / / MDVSA-2014:203 | Mandriva	MANDRIVA	w
About the security content of Xcode 7.0 - Apple Support	CONFIRM	s
OpenSSL SRTP and Session Ticket Memory Leaks Let Remote Users Deny Service - SecurityTracker	SECTRACK	w
Security Advisory SA62070 - NetBSD update for openssl - Secunia	SECUNIA	s
About Secunia Research | Flexera	SECUNIA	s
Red Hat Customer Portal	REDHAT	rh
About Secunia Research | Flexera	SECUNIA	s
Multiple Security Vulnerabilities in Citrix NetScaler Platform IPMI Lights Out Management (LOM) firmware	CONFIRM	s
Oracle Critical Patch Update - July 2015	CONFIRM	w
Red Hat Customer Portal	REDHAT	rh
'[security bulletin] HPSBGN03233 rev.1 - HP OneView running OpenSSL, Remote Denial of Service (DoS), ' - MARC	HP	m
APPLE-SA-2015-09-16-2 Xcode 7.0	APPLE	li
Multiple vulnerabilities in OpenSSL (Third Party Vulnerability Resolution Blog)	CONFIRM	b

www.openssl.org/news/secadv_20141015.txt	CONFIRM	w
IBM Security Bulletin: - United States	CONFIRM	w
'[security bulletin] HPSBMU03223 rev.1 - HP Insight Control server provisioning running SSLv3, Remote' - MARC	HP	m
About the security content of OS X Yosemite v10.10.2 and Security Update 2015-001 - Apple Support	CONFIRM	s
Document Display | HPE Support Center	CONFIRM	h
About Secunia Research | Flexera	SECUNIA	s
[security-announce] SUSE-SU-2014:1361-1: important: Security update for	SUSE	lis
USN-2385-1: OpenSSL vulnerabilities | Ubuntu	UBUNTU	w
Oracle Critical Patch Update - January 2015	CONFIRM	w
OpenSSL: Multiple vulnerabilities (GLSA 201412-39) — Gentoo Security	GENTOO	s
OpenSSL Session Ticket Memory Leak Remote Denial of Service Vulnerability	BID	w
'[security bulletin] HPSBMU03296 rev.1 - HP BladeSystem c-Class Onboard Administrator running OpenSSL' - MARC	HP	m
NetBSD-SA2014-015	NETBSD	ft
Support / Security / Advisories / / MDVSA-2015:062 | Mandriva	MANDRIVA	w
Security Advisory SA61298 - Mageia update for openssl - Secunia	SECUNIA	s
About Secunia Research | Flexera	SECUNIA	s
Security Advisory SA62030 - NetBSD update for openssl - Secunia	SECUNIA	s
Splunk Enterprise versions 6.0.7 and 5.0.11 address three vulnerabilities | Splunk	CONFIRM	w
About Secunia Research | Flexera	SECUNIA	s
[security-announce] openSUSE-SU-2014:1331-1: important: update for opens	SUSE	lis
git.openssl.org Git - openssl.git/commit	CONFIRM	g
'[security bulletin] HPSBOV03227 rev.1 - HP SSL for OpenVMS, Remote Disclosure of Information, Denial' - MARC	HP	m
Security Advisory SA61959 - IBM Tivoli Management Framework Multiple Vulnerabilities - Secunia	SECUNIA	s
[security-announce] SUSE-SU-2014:1357-1: important: Security update for	SUSE	lis
Security Advisory SA61837 - IBM AIX / Virtual I/O Server OpenSSL Two Denial of Service Vulnerabilities - Secunia	SECUNIA	s
About Secunia Research | Flexera	SECUNIA	s
'[security bulletin] HPSBMU03304 rev.1 - HP Insight Control server deployment on Linux and Windows, R' - MARC	HP	m
[security-announce] openSUSE-SU-2016:0640-1: important: Security update	SUSE	lis
aix.software.ibm.com/aix/efixes/security/openssl_advisory11.asc	CONFIRM	a
Document Display | HPE Support Center	CONFIRM	h
Security Advisory SA61990 - SUSE update for openssl - Secunia	SECUNIA	s
APPLE-SA-2015-01-27-4 OS X 10.10.2 and Security Update 2015-001	APPLE	lis
'[security bulletin] HPSBUX03162 SSRT101767 rev.1 - HP-UX Running OpenSSL, Remote Denial of Service (' - MARC	HP	m
About Secunia Research | Flexera	SECUNIA	s
'[security bulletin] HPSBHF03300 rev.1 - HP Network Products running OpenSSL, Remote Denial of Servic' - MARC	HP	m

'[security bulletin] HPSBMU03260 rev.1 - HP System Management Homepage running OpenSSL on Linux and W' - MARC	HP	m
git.openssl.org Git - openssl.git/commit		g
'[security bulletin] HPSBMU03261 rev.2 - HP Systems Insight Manager running OpenSSL on Linux and Wind' - MARC	HP	m
Debian -- Security Information -- DSA-3053-1 openssl	DEBIAN	w
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

390226 Oracle Managed Virtualization (VM) Server for x86 Security Update for Open Secure Sockets Layer (OpenSSL) (OVMSA-2021-0011)

390284 Oracle Managed Virtualization (VM) Server for x86 Security Update for Open Secure Sockets Layer (OpenSSL) (OVMSA-2023-0013)

591311 Bosch Rexroth PRA-ES8P2S Ethernet-Switch Multiple Vulnerabilities (BOSCH-SA-247053-BT)