



CVE-2014-3568

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2014-3568
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	OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j does not properly enforce the no-ssl3 build option, wh

Risk And Classification

Problem Types: CWE-310

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	Link
McAfee KnowledgeBase - McAfee Security Bulletin - Three SSLv3 Vulnerabilities	CONFIRM	k
'[security bulletin] HPSB MU03267 rev.1 - HP Matrix Operating Environment and HP CloudSystem Matrix ru' - MARC	HP	m
'[security bulletin] HPSB MU03263 rev.3 - HP Insight Control running OpenSSL, Remote Disclosure of Inf' - MARC	HP	m
About the security content of Xcode 7.0 - Apple Support	CONFIRM	s
Security Advisory SA62070 - NetBSD update for openssl - Secunia	SECUNIA	s
About Secunia Research Flexera	SECUNIA	s
About Secunia Research Flexera	SECUNIA	s
git.openssl.org Git - openssl.git/commit		g
Multiple Security Vulnerabilities in Citrix NetScaler Platform IPMI Lights Out Management (LOM) firmware	CONFIRM	s
OpenSSL 'no-ssl3' Build Option Security Bypass Vulnerability	BID	w
APPLE-SA-2015-09-16-2 Xcode 7.0	APPLE	li
[security-announce] SUSE-SU-2015:0578-1: important: Security update for	SUSE	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
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	li
IBM X-Force Exchange	XF	e
OpenSSL: Multiple vulnerabilities (GLSA 201412-39) — Gentoo Security	GENTOO	s
git.openssl.org Git - openssl.git/commit	CONFIRM	g
NetBSD-SA2014-015	NETBSD	ft
'[security bulletin] HPSBOV03227 rev.1 - HP SSL for OpenVMS, Remote Disclosure of Information, Denial' - MARC	HP	nr
About Secunia Research Flexera	SECUNIA	s
Security Advisory SA62030 - NetBSD update for openssl - Secunia	SECUNIA	s
About Secunia Research Flexera	SECUNIA	s
'[security bulletin] HPSBMU03260 rev.1 - HP System Management Homepage running OpenSSL on Linux and W' - MARC	HP	nr
[security-announce] openSUSE-SU-2014:1331-1: important: update for opens	SUSE	li
Security Advisory SA61959 - IBM Tivoli Management Framework Multiple Vulnerabilities - Secunia	SECUNIA	s
[security-announce] SUSE-SU-2014:1357-1: important: Security update for	SUSE	li
About Secunia Research Flexera	SECUNIA	s
'[security bulletin] HPSBMU03304 rev.1 - HP Insight Control server deployment on Linux and Windows, R' - MARC	HP	nr
[security-announce] openSUSE-SU-2016:0640-1: important: Security update	SUSE	li
Document Display HPE Support Center	CONFIRM	h
APPLE-SA-2015-01-27-4 OS X 10.10.2 and Security Update 2015-001	APPLE	li
'[security bulletin] HPSBUX03162 SSRT101767 rev.1 - HP-UX Running OpenSSL, Remote Denial of Service (' - MARC	HP	nr
About Secunia Research Flexera	SECUNIA	s
'[security bulletin] HPSBHF03300 rev.1 - HP Network Products running OpenSSL, Remote Denial of Servic' - MARC	HP	nr
OpenSSL 'no-ssl3' Build Option Fails to Prevent SSL 3.0 Handshakes - SecurityTracker	SECTRACK	w
'[security bulletin] HPSBMU03261 rev.2 - HP Systems Insight Manager running OpenSSL on Linux and Wind' - MARC	HP	nr
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

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

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](#)