



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

CVE	CVE-2009-3245
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-03-05 19:30:00 UTC
Updated	2026-04-29 01:13:23 UTC
Description	OpenSSL before 0.9.8m does not check for a NULL return value from bn_wexpand function calls in (1) crypto/bn/bn_div.c,

Primary CVSS: v2.0 10 from nvd@nist.gov

AV:N/AC:L/Au:N/C:C/I:C/A:C

Problem Types: CWE-20 | n/a

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Complete
Integrity	Complete
Availability	Complete
AV:N/AC:L/Au:N/C:C/I:C/A:C	

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	All	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References						
Reference						Source
Slackware update for openssl - Advisories - Community						af854a
ABB HMI Outdated Software Components ≈ Packet Storm						af854a
[security-announce] SUSE Security Summary Report: SUSE-SR:2010:013						af854a
'[CVS] OpenSSL: openssl/crypto/bn/ bn_div.c bn_gf2m.c openssl/crypto/ec...' - MARC						af854a
[SECURITY] Fedora 11 Update: openssl-0.9.8n-1.fc11						af854a
Repository / Oval Repository						af854a
Repository / Oval Repository						af854a
Fedora update for openssl - Advisories - Community						af854a
'[security bulletin] HPSBUX02517 SSRT100058 rev.1 - HP-UX Running OpenSSL, Remote Unauthorized Inform' - MARC						af854a
The Slackware Linux Project: Slackware Security Advisories						af854a
kb.bluecoat.com/index						af854a
About Secunia Research Flexera						af854a
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH						af854a
'[security bulletin] HPSBOV02540 SSRT090249 rev.1 - HP SSL for OpenVMS, Remote Unauthorized Data Inje' - MARC						af854a
[syslog-ng-announce] syslog-ng Premium Edition 3.0.6a has been released						af854a
Red Hat Customer Portal						af854a
OpenSSL TLS Session Renegotiation Plaintext Injection Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com						af854a
About the security content of Mac OS X v10.6.8 and Security Update 2011-004 - Apple Support						af854a

About the security content of Mac OS X v10.6.8 and Security Update 2011-004 - Apple Support	af854a
Repository / Oval Repository	af854a
aix.software.ibm.com/aix/efixes/security/openssl_advisory.asc	af854a
APPLE-SA-2011-06-23-1 Mac OS X v10.6.8 and Security Update 2011-004	af854a
About Secunia Research Flexera	af854a
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a
Security Advisories Mandriva Linux	af854a
'[CVS] OpenSSL: OpenSSL_1_0_0-stable: openssl/crypto/bn/ bn_div.c bn_gf...' - MARC	af854a
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a
[SECURITY] Fedora 13 Update: openssl-1.0.0-1.fc13	af854a
Support	af854a
OpenSSL 'bn_wexpend()' Error Handling Unspecified Vulnerability	af854a
[syslog-ng-announce] syslog-ng Premium Edition 3.2.1a has been released	af854a
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a
IBM AIX update for OpenSSL - Advisories - Community	af854a
USN-1003-1: OpenSSL vulnerabilities Ubuntu	af854a
'[CVS] OpenSSL: OpenSSL_0_9_8-stable: openssl/ CHANGES openssl/crypto/b...' - MARC	af854a
CVE Program record	CVE.O
NVD vulnerability detail	NVD



Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2010-03-25	Vincent Danen	Red Hat is aware of this issue and is tracking it via the following bug: https://bugzilla.redhat.com/show_bug.cgi?id=544444



There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)