



CVE-2007-3108

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

Summary

CVE	CVE-2007-3108
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-08-08 01:17:00 UTC
Updated	2018-10-16 16:47:00 UTC
Description	The BN_from_montgomery function in crypto/bn/bn_mont.c in OpenSSL 0.9.8e and earlier does not properly perform Mont

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openssl	Openssl	All	All	All	All

References

Reference

- VUPEN Security - Offensive Cyber Security
- rPath update for openssl - Advisories - Secunia
- VMware ESXi OpenSSL Vulnerabilities - Advisories - Secunia
- USN-522-1: openssl vulnerabilities | Ubuntu security notices
- rhn.redhat.com | Red Hat Support
- VU#724968 - RSA key reconstruction vulnerability
- VMSA-2008-0001.1 - VMware
- VMware ESX Server Multiple Security Updates - Advisories - Secunia
- SecurityFocus
- Security Advisories | Mandriva Linux
- Debian -- Security Information -- DSA-1571-1 openssl
- rPath update for openssl - Advisories - Secunia
- VMSA-2008-0013.3 - VMware

Repository / Oval Repository
[Security-announce] VMSA-2008-0001 Moderate OpenPegasus PAM Authentication Buffer Overflow and updated service console packages
issues.rpath.com/browse/RPL-1633
Webmail - OVH
Webmail - OVH
Mandriva update for openssl - Advisories - Secunia
ASA-2007-485 (RHSA-2007-0813)
issues.rpath.com/browse/RPL-1613
SecurityFocus
OpenSSL RSA key reconstruction vulnerability (CVE-2007-3108, VU#724968) Blue Coat Systems, Inc.
Linux Terminal Server Project: Multiple vulnerabilities — Gentoo Linux Documentation
support.attachmate.com/techdocs/2374.html
Webmail - OVH
Red Hat update for openssl - Advisories - Secunia
Webmail - OVH
Blue Coat Products OpenSSL RSA Key Reconstruction Weakness - Advisories - Secunia
VMware updates for OpenSSL, net-snmp, and perl - Secunia Advisories - Vulnerability Intelligence - Secunia.com
/err404.html
Webmail - OVH
rhn.redhat.com Red Hat Support
Avaya Products OpenSSL Vulnerabilities - Advisories - Secunia
OpenSSL: CVS Web Interface
SecurityFocus
Gentoo Itsp Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com
Gentoo update for openssl - Advisories - Secunia
Ubuntu update for openssl - Advisories - Secunia
Reflection for Secure IT Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com
Gentoo Linux Documentation -- OpenSSL: Multiple vulnerabilities
Debian OpenSSL Predictable Random Number Generator and Update - Secunia Advisories - Vulnerability Information - Secunia.com
OpenSSL Montgomery Exponentiation Side-Channel Local Information Disclosure Vulnerability
Red Hat update for openssl - Advisories - Secunia
rhn.redhat.com Red Hat Support
OpenSSL Information for VU#724968
CVE Program record
NVD vulnerability detail

Vendor Comments And Credit

Organization	Published	Contributor	Statement
--------------	-----------	-------------	-----------

Red Hat	2007-08-14	Mark J Cox	This paper describes a possible side-channel attack that hasn't been proven outside of a lab env
---------	------------	------------	--

Legacy QID Mappings

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

© [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](#).

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