



CVE-2007-5502

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

Summary

CVE	CVE-2007-5502
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-12-01 06:46:00 UTC
Updated	2017-07-29 01:33:00 UTC
Description	The PRNG implementation for the OpenSSL FIPS Object Module 1.1.1 does not perform auto-seeding during the FIPS self

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openssl	Fips Object Module	1.1.1	All	All	All
Application	Openssl	Fips Object Module	1.1.1	All	All	All

References

Reference

- Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
- OpenSSL FIPS Object Module PRNG Seed Vulnerability
- US-CERT Vulnerability Note VU#150249
- OpenSSL FIPS Object Module PRNG Security Issue - Advisories - Secunia
- www.openssl.org/news/secadv_20071129.txt
- IBM X-Force Exchange
- SecurityTracker.com Archives - OpenSSL FIPS Object Module Self-Test Error Causes the System to Generate More Predictable Pseudo Ran
- CVE Program record
- NVD vulnerability detail

Vendor Comments And Credit

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

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](#).

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