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

Red Hat	2007-12-03	Mark J Cox	Not vulnerable. This vulnerability only affected the OpenSSL FIPS Object Module which is not e

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