CVE-2010-1633

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2010-1633
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-06-03 14:30:00 UTC
Updated	2023-11-07 02:05:00 UTC
Description	RSA verification recovery in the EVP_PKEY_verify_recover function in OpenSSL 1.x before 1.0.0a, as used by pkeyutl and

Risk And Classification

Problem Types: CWE-264

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	1.0.0	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

References

Reference	Source	Link
Security Advisory SA57353 - IBM Storage System DS8870 OpenSSL Multiple Vulnerabilities - Secunia	SECUNIA	secunia.com
IBM Security Bulletin: Storage HMC OpenSSL upgrade to address cryptographic vulnerabilities. - United States	CONFIRM	www-01.ibm.c

cvs.openssl.org/filediff	CONFIRM	cvs.openssl.or
cvs.openssl.org/chngview	CONFIRM	cvs.openssl.or
OpenSSL Two Vulnerabilities - Advisories - Community	SECUNIA	secunia.com
www.openssl.org/news/secadv_20100601.txt	CONFIRM	www.openssl.(
OpenSSL 'EVP_PKEY_verify_recover()' Invalid Return Value Security Bypass Vulnerability	BID	www.securityf(
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.cc
Bug 598732 – CVE-2010-1633 openssl: information leak due to invalid Return value check	CONFIRM	bugzilla.redha
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

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