CVE-2012-2686

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2012-2686
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-02-08 19:55:00 UTC
Updated	2023-11-07 02:10:00 UTC
Description	crypto/evp/e_aes_cbc_hmac_sha1.c in the AES-NI functionality in the TLS 1.1 and 1.2 implementations in OpenSSL 1.0.1

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openssl	Openssl	1.0.1	All	All	All
Application	Openssl	Openssl	1.0.1a	All	All	All
Application	Openssl	Openssl	1.0.1b	All	All	All
Application	Openssl	Openssl	1.0.1c	All	All	All
Application	Openssl	Openssl	1.0.1	All	All	All
Application	Openssl	Openssl	1.0.1a	All	All	All
Application	Openssl	Openssl	1.0.1b	All	All	All
Application	Openssl	Openssl	1.0.1c	All	All	All

References

Reference
OpenSSL CVE-2012-2686 Remote Denial of Service Vulnerability
git.openssl.org Git - openssl.git/commit
APPLE-SA-2013-09-12-1 OS X Mountain Lion v10.8.5 and Security Update 2013-004
Security Advisory SA55108 - IBM Tivoli Storage Productivity Center Multiple Vulnerabilities - Secunia
/err404.html
Repository / Oval Repository

git.openssl.org Git - openssl.git/commit
About the security content of OS X Mountain Lion v10.8.5 and Security Update 2013-004
Repository / Oval Repository
Bug 908029 – CVE-2012-2686 openssl: DoS due to improper handling of CBC ciphersuites in TLS 1.1/1.2 on AES-NI supporting platforms
Security Advisory SA55139 - IBM Initiate Master Data Service / InfoSphere Master Data Management OpenSSL Vulnerabilities - Secunia
'[security bulletin] HPSBUX02909 SSRT101289 rev.1 - HP-UX Apache Web Server, Remote Denial of Service' - MARC
Document Display | HPE Support Center
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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