



CVE-2010-0740

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

Summary

CVE	CVE-2010-0740
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-03-26 18:30:00 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The ssl3_get_record function in ssl/s3_pkt.c in OpenSSL 0.9.8f through 0.9.8m allows remote attackers to cause a denial of service (CPU consumption) via a crafted TLS record.

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:N/I:N/A:P

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:L/Au:N/C:N/I:N/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openssl	Openssl	0.9.8f	All	All	All

Application	Openssl	Openssl	0.9.8g	All	All	All
Application	Openssl	Openssl	0.9.8h	All	All	All
Application	Openssl	Openssl	0.9.8i	All	All	All
Application	Openssl	Openssl	0.9.8j	All	All	All
Application	Openssl	Openssl	0.9.8k	All	All	All
Application	Openssl	Openssl	0.9.8l	All	All	All
Application	Openssl	Openssl	0.9.8m	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References	
Reference	Source
SecurityFocus	af854a3a-2127-4
VMware vCenter Server 4.1 Update 1 Release Notes	af854a3a-2127-4
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-4
'[security bulletin] HPSBUX02517 SSRT100058 rev.1 - HP-UX Running OpenSSL, Remote Unauthorized Inform' - MARC	af854a3a-2127-4
kb.bluecoat.com/index	af854a3a-2127-4
About Secunia Research Flexera	af854a3a-2127-4
www.openssl.org/news/secadv_20100324.txt	af854a3a-2127-4
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-4
VMSA-2011-0003	af854a3a-2127-4
VMware vCenter Server OpenSSL Denial of Service Vulnerabilities - Advisories - Community	af854a3a-2127-4
[syslog-ng-announce] syslog-ng Premium Edition 3.0.6a has been released	af854a3a-2127-4
About the security content of Mac OS X v10.6.8 and Security Update 2011-004 - Apple Support	af854a3a-2127-4
Repository / Oval Repository	af854a3a-2127-4
aix.software.ibm.com/aix/efixes/security/openssl_advisory.asc	af854a3a-2127-4
APPLE-SA-2011-06-23-1 Mac OS X v10.6.8 and Security Update 2011-004	af854a3a-2127-4
SecurityTracker.com Archives - OpenSSL Record Processing Bug Lets Remote Users Deny Service	af854a3a-2127-4
About Secunia Research Flexera	af854a3a-2127-4
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-4
Security Advisories Mandriva Linux	af854a3a-2127-4
[SECURITY] Fedora 13 Update: openssl-1.0.0-1.fc13	af854a3a-2127-4
[syslog-ng-announce] syslog-ng Premium Edition 3.2.1a has been released	af854a3a-2127-4
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-4
'[security bulletin] HPSBUX02517 SSRT100108 rev.1 - HP-UX Running Apache-based Web Server, Remote Denial of Service' - MARC	af854a3a-2127-4

[security bulletin] HP-UX Running Apache-based web Server, Remote Deni - MARC	af854a3a-2127-4
IBM AIX update for OpenSSL - Advisories - Community	af854a3a-2127-4
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2010-03-27	Vincent Danen	Not vulnerable. This issue did not affect the versions of openssl as shipped with Red Hat Ente

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