CVE-2016-7055

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

Summary

CVE	CVE-2016-7055
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-05-04 20:29:00 UTC
Updated	2022-09-01 16:25:00 UTC
Description	There is a carry propagating bug in the Broadwell-specific Montgomery multiplication procedure in OpenSSL 1.0.2 and 1.1.(

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nodejs	Node.js	All	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Openssl	Openssl	All	All	All	All
Application	Openssl	Openssl	All	All	All	All

References

Reference	Source	Link
OpenSSL: Multiple vulnerabilities (GLSA 201702-07) — Gentoo Security	GENTOO	security.gentoo.org
www.openssl.org/news/secadv/20161110.txt	CONFIRM	www.openssl.org
FreeBSD-SA-17:02	FREEBSD	security.FreeBSD.org
Oracle Critical Patch Update - January 2018	CONFIRM	www.oracle.com
OpenSSL Multiple Bugs Let Remote Users Cause the Target Application to Crash - SecurityTracker	SECTRACK	www.securitytracker.c
[R5] SecurityCenter 5.4.3 Fixes Multiple Vulnerabilities - Security Advisory | Tenable Network Security	CONFIRM	www.tenable.com
Document Display | HPE Support Center	CONFIRM	h20566.www2.hpe.co
Red Hat Customer Portal	REDHAT	access.redhat.com

Red Hat Customer Portal	REDHAT	access.redhat.com
OpenSSL CVE-2016-7055 Denial of Service Vulnerability	BID	www.securityfocus.co
Red Hat Customer Portal	REDHAT	access.redhat.com
Document Display | HPE Support Center	CONFIRM	h20566.www2.hpe.co
Oracle Critical Patch Update - July 2017	CONFIRM	www.oracle.com
Oracle Critical Patch Update - October 2017	CONFIRM	www.oracle.com
Oracle Critical Patch Update Advisory - April 2019	MISC	www.oracle.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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