CVE-2021-4160

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-4160
State	PUBLIC
Assigner	openssl-security@openssl.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-28 22:15:00 UTC
Updated	2023-11-07 03:40:00 UTC
Description	There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, includi

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Openssl	Openssl	All	All	All	All
Application	Openssl	Openssl	1.0.2	-	All	All
Application	Openssl	Openssl	1.0.2	beta1	All	All
Application	Openssl	Openssl	1.0.2	beta2	All	All
Application	Openssl	Openssl	1.0.2	beta3	All	All
Application	Openssl	Openssl	1.0.2a	All	All	All
Application	Openssl	Openssl	1.0.2b	All	All	All
Application	Openssl	Openssl	1.0.2c	All	All	All
Application	Openssl	Openssl	1.0.2d	All	All	All
Application	Openssl	Openssl	1.0.2e	All	All	All
Application	Openssl	Openssl	1.0.2f	All	All	All
Application	Openssl	Openssl	1.0.2g	All	All	All
Application	Openssl	Openssl	1.0.2h	All	All	All
Application	Openssl	Openssl	1.0.2i	All	All	All

Application	Openssl	Openssl	1.0.2j	All	All	All
Application	Openssl	Openssl	1.0.2k	All	All	All
Application	Openssl	Openssl	1.0.2l	All	All	All
Application	Openssl	Openssl	1.0.2m	All	All	All
Application	Openssl	Openssl	1.0.2n	All	All	All
Application	Openssl	Openssl	1.0.2o	All	All	All
Application	Openssl	Openssl	1.0.2p	All	All	All
Application	Openssl	Openssl	1.0.2q	All	All	All
Application	Openssl	Openssl	1.0.2r	All	All	All
Application	Openssl	Openssl	1.0.2s	All	All	All
Application	Openssl	Openssl	1.0.2t	All	All	All
Application	Openssl	Openssl	1.0.2u	All	All	All
Application	Openssl	Openssl	1.0.2v	All	All	All
Application	Openssl	Openssl	1.0.2w	All	All	All
Application	Openssl	Openssl	1.0.2x	All	All	All
Application	Openssl	Openssl	1.0.2y	All	All	All
Application	Openssl	Openssl	1.0.2za	All	All	All
Application	Openssl	Openssl	1.0.2zb	All	All	All
Application	Openssl	Openssl	1.1.1	-	All	All
Application	Openssl	Openssl	1.1.1	pre1	All	All
Application	Openssl	Openssl	1.1.1	pre2	All	All
Application	Openssl	Openssl	1.1.1	pre3	All	All
Application	Openssl	Openssl	1.1.1	pre4	All	All
Application	Openssl	Openssl	1.1.1	pre5	All	All
Application	Openssl	Openssl	1.1.1	pre6	All	All
Application	Openssl	Openssl	1.1.1	pre7	All	All
Application	Openssl	Openssl	1.1.1	pre8	All	All
Application	Openssl	Openssl	1.1.1	pre9	All	All
Application	Openssl	Openssl	1.1.1a	All	All	All
Application	Openssl	Openssl	1.1.1b	All	All	All
Application	Openssl	Openssl	1.1.1c	All	All	All
Application	Openssl	Openssl	1.1.1d	All	All	All
Application	Openssl	Openssl	1.1.1e	All	All	All
Application	Openssl	Openssl	1.1.1f	All	All	All
Application	Openssl	Openssl	1.1.1g	All	All	All

Application	Openssl	Openssl	1.1.1h	All	All	All
Application	Openssl	Openssl	1.1.1i	All	All	All
Application	Openssl	Openssl	1.1.1j	All	All	All
Application	Openssl	Openssl	1.1.1k	All	All	All
Application	Openssl	Openssl	1.1.1l	All	All	All
Application	Openssl	Openssl	3.0.0	-	All	All
Application	Openssl	Openssl	3.0.0	alpha1	All	All
Application	Openssl	Openssl	3.0.0	alpha10	All	All
Application	Openssl	Openssl	3.0.0	alpha11	All	All
Application	Openssl	Openssl	3.0.0	alpha12	All	All
Application	Openssl	Openssl	3.0.0	alpha13	All	All
Application	Openssl	Openssl	3.0.0	alpha14	All	All
Application	Openssl	Openssl	3.0.0	alpha15	All	All
Application	Openssl	Openssl	3.0.0	alpha16	All	All
Application	Openssl	Openssl	3.0.0	alpha17	All	All
Application	Openssl	Openssl	3.0.0	alpha2	All	All
Application	Openssl	Openssl	3.0.0	alpha3	All	All
Application	Openssl	Openssl	3.0.0	alpha4	All	All
Application	Openssl	Openssl	3.0.0	alpha5	All	All
Application	Openssl	Openssl	3.0.0	alpha6	All	All
Application	Openssl	Openssl	3.0.0	alpha7	All	All
Application	Openssl	Openssl	3.0.0	alpha8	All	All
Application	Openssl	Openssl	3.0.0	alpha9	All	All
Application	Openssl	Openssl	3.0.0	beta1	All	All
Application	Openssl	Openssl	3.0.0	beta2	All	All
Application	Openssl	Openssl	All	All	All	All
Application	Oracle	Enterprise Manager Ops Center	12.4.0.0	All	All	All
Application	Oracle	Health Sciences Inform Publisher	6.2.1.1	All	All	All
Application	Oracle	Health Sciences Inform Publisher	6.3.1.1	All	All	All
Application	Oracle	Jd Edwards Enterpriseone Tools	9.2.6.3	All	All	All
Application	Oracle	Jd Edwards World Security	a9.4	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.58	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.59	All	All	All
Application	Siemens	Sinec Ins	All	All	All	All
Application	Siemens	Sinec Ins	1.0	-	All	All

Application	Siemens	Sinec Ins	1.0	sp1	All	All

References

Reference	Source	Link	Tags
www.openssl.org/news/secadv/20220128.txt	CONFIRM	www.openssl.org	
git.openssl.org Git - openssl.git/commitdiff	CONFIRM	git.openssl.org	
git.openssl.org Git - openssl.git/commitdiff	CONFIRM	git.openssl.org	
Oracle Critical Patch Update Advisory - April 2022	MISC	www.oracle.com	
OpenSSL: Multiple Vulnerabilities (GLSA 202210-02) — Gentoo security	GENTOO	security.gentoo.org	
cert-portal.siemens.com/productcert/pdf/ssa-637483.pdf	CONFIRM	cert-portal.siemens.com	
git.openssl.org Git - openssl.git/commitdiff		git.openssl.org	
git.openssl.org Git - openssl.git/commitdiff	CONFIRM	git.openssl.org	
Debian -- Security Information -- DSA-5103-1 openssl	DEBIAN	www.debian.org	
git.openssl.org Git - openssl.git/commitdiff		git.openssl.org	
git.openssl.org Git		git.openssl.org	
Oracle Critical Patch Update Advisory - July 2022	N/A	www.oracle.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: Bernd Edlinger

Legacy QID Mappings

- 179142 Debian Security Update for Open Secure Sockets Layer (OpenSSL) (DSA 5103-1)
- 181942 Debian Security Update for Open Secure Sockets Layer (OpenSSL) (CVE-2021-4160)
- 376547 Oracle PeopleSoft Enterprise PeopleTools Product Multiple Vulnerabilities (CPUAPR2022)
- 379452 IBM Cognos Analytics Multiple Vulnerabilities (7123154)
- 591311 Bosch Rexroth PRA-ES8P2S Ethernet-Switch Multiple Vulnerabilities (BOSCH-SA-247053-BT)
- 671446 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2022-1455)
- 671457 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2022-1434)
- 671618 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2022-1649)
- 671628 EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2022-1663)
- 690776 Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) (1aaaa5c6-804d-

11ec-8be6-d4c9ef517024)

710638 Gentoo Linux Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (GLSA 202210-02)

900646 Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (8471)

901843 Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (8472-1)

906136 Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (8471-1)

906392 Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (8472-2)