CVE-2022-2274

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-2274
State	PUBLIC
Assigner	openssl-security@openssl.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-07-01 08:15:00 UTC
Updated	2023-11-07 03:46:00 UTC
Description	The OpenSSL 3.0.4 release introduced a serious bug in the RSA implementation for X86_64 CPUs supporting the AVX512

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Netapp	H300s	-	All	All	All
Operating System	Netapp	H300s Firmware	-	All	All	All
Hardware	Netapp	H410c	-	All	All	All
Operating System	Netapp	H410c Firmware	-	All	All	All
Hardware	Netapp	H410s	-	All	All	All
Operating System	Netapp	H410s Firmware	-	All	All	All
Hardware	Netapp	H500s	-	All	All	All
Operating System	Netapp	H500s Firmware	-	All	All	All
Hardware	Netapp	H700s	-	All	All	All
Operating System	Netapp	H700s Firmware	-	All	All	All
Application	Netapp	Snapcenter	-	All	All	All
Application	Openssl	Openssl	3.0.4	All	All	All

References

Reference	Source	Link	Tags
git.openssl.org Git		git.openssl.org	
git.openssl.org Git - openssl.git/commitdiff	CONFIRM	git.openssl.org	

www.openssl.org/news/secadv/20220705.txt	CONFIRM	www.openssl.org	
AVX512-specific heap buffer overflow with 3.0.4 release · Issue #18625 · openssl/openssl · GitHub	CONFIRM	github.com	
CVE-2022-2274 OpenSSL Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	
git.openssl.org Git - openssl.git/commitdiff	MITRE	git.openssl.org	
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

182609 Debian Security Update for Open Secure Sockets Layer (OpenSSL) (CVE-2022-2274)

296084 Oracle Solaris 11.4 Support Repository Update (SRU) 50.126.3 Missing (CPUOCT2022)

377911 Oracle Hypertext Transfer Protocol Server (HTTP Server) Multiple Vulnerabilities (CPUJAN2023)

38874 OpenSSL Heap Memory Corruption Vulnerability

591406 Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)

690890 Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) (f0e45968-faff-11ec-856e-d4c9ef517024)