CVE-2018-0733

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-0733
State	PUBLIC
Assigner	openssl-security@openssl.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-03-27 21:29:00 UTC
Updated	2023-11-07 02:51:00 UTC
Description	Because of an implementation bug the PA-RISC CRYPTO_memcmp function is effectively reduced to only comparing the l

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
OpenSSL CVE-2018-0733 Security Bypass Vulnerability	BID	www.sec
git.openssl.org Git - openssl.git/commitdiff	CONFIRM	git.opens
OpenSSL: Multiple vulnerabilities (GLSA 201811-21) — Gentoo security	GENTOO	security.g
CPU July 2018	CONFIRM	www.ora
March 2018 OpenSSL Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.r
git.openssl.org Git - openssl.git/commitdiff		git.opens
www.openssl.org/news/secadv/20180327.txt	CONFIRM	www.ope
[R1] Nessus Network Monitor 5.5.0 Fixes One Third-party Vulnerability - Security Advisory | Tenable®	CONFIRM	www.ten
Oracle Critical Patch Update - January 2019	CONFIRM	www.ora
Oracle Critical Patch Update - July 2019	MISC	www.ora
[R1] Industrial Security 1.1.0 Fixes One Third-party Vulnerability - Security Advisory | Tenable®	CONFIRM	www.ten
OpenSSL Bugs Let Users Deny Service and Bypass Authentication in Certain Cases - SecurityTracker	SECTRACK	www.sec
CPU Oct 2018	CONFIRM	www.ora

[R1] OpenSSL Stand-alone Patch Available for SecurityCenter versions 5.0 or Later - Security Advisory | Tenable®	CONFIRM	www.ten
Oracle Critical Patch Update Advisory - April 2019	MISC	www.ora
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

Vendor Comments And Credit

Discovery Credit

LEGACY: Peter Waltenberg (IBM)

Legacy QID Mappings

710214 Gentoo Linux Open Secure Sockets Layer Multiple Vulnerabilities (GLSA 201811-21)