CVE-2020-16088

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-16088
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-07-28 12:15:00 UTC
Updated	2022-01-04 16:32:00 UTC
Description	iked in OpenIKED, as used in OpenBSD through 6.7, allows authentication bypass because ca.c has the wrong logic for ch

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Openbsd	Openbsd	All	All	All	All

References

Reference	Source	Link	T
OpenIKED Security	MISC	www.openiked.org	V
ftp.openbsd.org/pub/OpenBSD/patches/6.7/common/014_iked.patch.sig	CONFIRM	ftp.openbsd.org	E
Fix return value check for openssl API used during pubkey validation. · openbsd/src@7afb2d4 · GitHub	MISC	github.com	
Commits · xcllnt/openiked · GitHub	MISC	github.com	P
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

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

CVE.report and Source URL Uptime Status status.cve.report