



# CVE-2020-16088

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2020-16088
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-07-28 12:15:00 UTC
<b>Updated</b>	2022-01-04 16:32:00 UTC
<b>Description</b>	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	<a href="http://www.openiked.org">www.openiked.org</a>	V
<a href="ftp://openbsd.org/pub/OpenBSD/patches/6.7/common/014_iked.patch.sig">ftp.openbsd.org/pub/OpenBSD/patches/6.7/common/014_iked.patch.sig</a>	CONFIRM	<a href="ftp://openbsd.org">ftp.openbsd.org</a>	E
Fix return value check for openssl API used during pubkey validation. · openbsd/src@7afb2d4 · GitHub	MISC	<a href="https://github.com">github.com</a>	
Commits · xclnt/openiked · GitHub	MISC	<a href="https://github.com">github.com</a>	P
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	ca
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	ca

No vendor comments have been submitted for this CVE.

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

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**