



CVE-2010-4478

Published on: 12/06/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:01 PM UTC

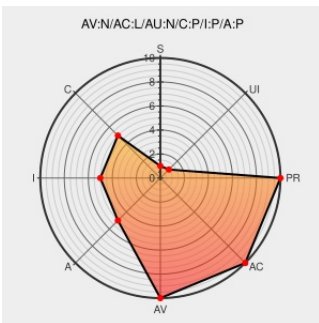
CVE-2010-4478

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Openssh](#) from [Openbsd](#) contain the following vulnerability:

OpenSSH 5.6 and earlier, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol, a related issue to CVE-2010-4252.

CVE-2010-4478 has been assigned by [M cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References


Description	Tags	Link
Error	Patch www.openbsd.org text/html Inactive Link Not Archived	CONFIRM www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/jpake.c.diff?r1=1.4;r2=1.5;f=h
GitHub - seb-m/jpake: Small-subgroup confinement issue in the OpenSSL and OpenSSH implementations of J-PAKE.	github.com text/html	MISC github.com/seb-m/jpake
CVS log for src/usr.bin/ssh/jpake.c	Patch www.openbsd.org text/html	CONFIRM www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/jpake.c#rev1.5
Bug 659297 – CVE-2010-4252 openssl: session key retrieval flaw in J-PAKE implementation	Patch bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=659297

Repository / Oval Repository

[oval.cisecurity.org](https://oval.cisecurity.org/text/html)
text/html

 OVAL oval.org/mitre.oval:def:12338

Exploit
seb.dbzteam.org
application/pdf

 MISC seb.dbzteam.org/crypto/jpake-session-key-retrieval.pdf

Juniper Networks - 2015-04 Security Bulletin: IDP: Multiple vulnerabilities addressed by third party software updates.

kb.juniper.net
text/html

 CONFIRM
kb.juniper.net/InfoCenter/index?page=content&id=JSA10673

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openbsd	Openssh	1.2	All	All	All
Application	Openbsd	Openssh	1.2.1	All	All	All
Application	Openbsd	Openssh	1.2.2	All	All	All
Application	Openbsd	Openssh	1.2.27	All	All	All
Application	Openbsd	Openssh	1.2.3	All	All	All
Application	Openbsd	Openssh	1.3	All	All	All
Application	Openbsd	Openssh	1.5	All	All	All
Application	Openbsd	Openssh	1.5.7	All	All	All
Application	Openbsd	Openssh	1.5.8	All	All	All
Application	Openbsd	Openssh	2.1	All	All	All
Application	Openbsd	Openssh	2.1.1	All	All	All
Application	Openbsd	Openssh	2.2	All	All	All
Application	Openbsd	Openssh	2.3	All	All	All
Application	Openbsd	Openssh	2.3.1	All	All	All
Application	Openbsd	Openssh	2.5	All	All	All
Application	Openbsd	Openssh	2.5.1	All	All	All
Application	Openbsd	Openssh	2.5.2	All	All	All
Application	Openbsd	Openssh	2.9	All	All	All
Application	Openbsd	Openssh	2.9.9	All	All	All
Application	Openbsd	Openssh	2.9.9p2	All	All	All
Application	Openbsd	Openssh	2.9p1	All	All	All
Application	Openbsd	Openssh	2.9p2	All	All	All

Application	Openbsd	Openssh	3.0	All	All	All
Application	Openbsd	Openssh	3.0.1	All	All	All
Application	Openbsd	Openssh	3.0.1p1	All	All	All
Application	Openbsd	Openssh	3.0.2	All	All	All
Application	Openbsd	Openssh	3.0.2p1	All	All	All
Application	Openbsd	Openssh	3.0p1	All	All	All
Application	Openbsd	Openssh	3.1	All	All	All
Application	Openbsd	Openssh	3.1p1	All	All	All
Application	Openbsd	Openssh	3.2	All	All	All
Application	Openbsd	Openssh	3.2.2	All	All	All
Application	Openbsd	Openssh	3.2.2p1	All	All	All
Application	Openbsd	Openssh	3.2.3p1	All	All	All
Application	Openbsd	Openssh	3.3	All	All	All
Application	Openbsd	Openssh	3.3p1	All	All	All
Application	Openbsd	Openssh	3.4	All	All	All
Application	Openbsd	Openssh	3.4p1	All	All	All
Application	Openbsd	Openssh	3.5	All	All	All
Application	Openbsd	Openssh	3.5p1	All	All	All
Application	Openbsd	Openssh	3.6	All	All	All
Application	Openbsd	Openssh	3.6.1	All	All	All
Application	Openbsd	Openssh	3.6.1p1	All	All	All
Application	Openbsd	Openssh	3.6.1p2	All	All	All
Application	Openbsd	Openssh	3.7	All	All	All
Application	Openbsd	Openssh	3.7.1	All	All	All
Application	Openbsd	Openssh	3.7.1p1	All	All	All
Application	Openbsd	Openssh	3.7.1p2	All	All	All
Application	Openbsd	Openssh	3.8	All	All	All
Application	Openbsd	Openssh	3.8.1	All	All	All
Application	Openbsd	Openssh	3.8.1p1	All	All	All
Application	Openbsd	Openssh	3.9	All	All	All
Application	Openbsd	Openssh	3.9.1	All	All	All
Application	Openbsd	Openssh	3.9.1p1	All	All	All
Application	Openbsd	Openssh	4.0	All	All	All
Application	Openbsd	Openssh	4.0p1	All	All	All
Application	Openbsd	Openssh	4.1	All	All	All

Application	Openbsd	Openssh	4.1p1	All	All	All
Application	Openbsd	Openssh	4.2	All	All	All
Application	Openbsd	Openssh	4.2p1	All	All	All
Application	Openbsd	Openssh	4.3	All	All	All
Application	Openbsd	Openssh	4.3p1	All	All	All
Application	Openbsd	Openssh	4.3p2	All	All	All
Application	Openbsd	Openssh	4.4	All	All	All
Application	Openbsd	Openssh	4.4p1	All	All	All
Application	Openbsd	Openssh	4.5	All	All	All
Application	Openbsd	Openssh	4.6	All	All	All
Application	Openbsd	Openssh	4.7	All	All	All
Application	Openbsd	Openssh	4.7p1	All	All	All
Application	Openbsd	Openssh	4.8	All	All	All
Application	Openbsd	Openssh	4.9	All	All	All
Application	Openbsd	Openssh	5.0	All	All	All
Application	Openbsd	Openssh	5.1	All	All	All
Application	Openbsd	Openssh	5.2	All	All	All
Application	Openbsd	Openssh	5.3	All	All	All
Application	Openbsd	Openssh	5.4	All	All	All
Application	Openbsd	Openssh	5.5	All	All	All
Application	Openbsd	Openssh	1.2	All	All	All
Application	Openbsd	Openssh	1.2.1	All	All	All
Application	Openbsd	Openssh	1.2.2	All	All	All
Application	Openbsd	Openssh	1.2.27	All	All	All
Application	Openbsd	Openssh	1.2.3	All	All	All
Application	Openbsd	Openssh	1.3	All	All	All
Application	Openbsd	Openssh	1.5	All	All	All
Application	Openbsd	Openssh	1.5.7	All	All	All
Application	Openbsd	Openssh	1.5.8	All	All	All
Application	Openbsd	Openssh	2.1	All	All	All
Application	Openbsd	Openssh	2.1.1	All	All	All
Application	Openbsd	Openssh	2.2	All	All	All
Application	Openbsd	Openssh	2.3	All	All	All
Application	Openbsd	Openssh	2.3.1	All	All	All
Application	Openbsd	Openssh	2.5	All	All	All

Application	Openbsd	Openssh	2.5.1	All	All	All
Application	Openbsd	Openssh	2.5.2	All	All	All
Application	Openbsd	Openssh	2.9	All	All	All
Application	Openbsd	Openssh	2.9.9	All	All	All
Application	Openbsd	Openssh	2.9.9p2	All	All	All
Application	Openbsd	Openssh	2.9p1	All	All	All
Application	Openbsd	Openssh	2.9p2	All	All	All
Application	Openbsd	Openssh	3.0	All	All	All
Application	Openbsd	Openssh	3.0.1	All	All	All
Application	Openbsd	Openssh	3.0.1p1	All	All	All
Application	Openbsd	Openssh	3.0.2	All	All	All
Application	Openbsd	Openssh	3.0.2p1	All	All	All
Application	Openbsd	Openssh	3.0p1	All	All	All
Application	Openbsd	Openssh	3.1	All	All	All
Application	Openbsd	Openssh	3.1p1	All	All	All
Application	Openbsd	Openssh	3.2	All	All	All
Application	Openbsd	Openssh	3.2.2	All	All	All
Application	Openbsd	Openssh	3.2.2p1	All	All	All
Application	Openbsd	Openssh	3.2.3p1	All	All	All
Application	Openbsd	Openssh	3.3	All	All	All
Application	Openbsd	Openssh	3.3p1	All	All	All
Application	Openbsd	Openssh	3.4	All	All	All
Application	Openbsd	Openssh	3.4p1	All	All	All
Application	Openbsd	Openssh	3.5	All	All	All
Application	Openbsd	Openssh	3.5p1	All	All	All
Application	Openbsd	Openssh	3.6	All	All	All
Application	Openbsd	Openssh	3.6.1	All	All	All
Application	Openbsd	Openssh	3.6.1p1	All	All	All
Application	Openbsd	Openssh	3.6.1p2	All	All	All
Application	Openbsd	Openssh	3.7	All	All	All
Application	Openbsd	Openssh	3.7.1	All	All	All
Application	Openbsd	Openssh	3.7.1p1	All	All	All
Application	Openbsd	Openssh	3.7.1p2	All	All	All
Application	Openbsd	Openssh	3.8	All	All	All
Application	Openbsd	Openssh	3.8.1	All	All	All
Application	Openbsd	Openssh	3.8.1p1	All	All	All

Application	Openbsd	Openssh	3.9	All	All	All
Application	Openbsd	Openssh	3.9.1	All	All	All
Application	Openbsd	Openssh	3.9.1p1	All	All	All
Application	Openbsd	Openssh	4.0	All	All	All
Application	Openbsd	Openssh	4.0p1	All	All	All
Application	Openbsd	Openssh	4.1	All	All	All
Application	Openbsd	Openssh	4.1p1	All	All	All
Application	Openbsd	Openssh	4.2	All	All	All
Application	Openbsd	Openssh	4.2p1	All	All	All
Application	Openbsd	Openssh	4.3	All	All	All
Application	Openbsd	Openssh	4.3p1	All	All	All
Application	Openbsd	Openssh	4.3p2	All	All	All
Application	Openbsd	Openssh	4.4	All	All	All
Application	Openbsd	Openssh	4.4p1	All	All	All
Application	Openbsd	Openssh	4.5	All	All	All
Application	Openbsd	Openssh	4.6	All	All	All
Application	Openbsd	Openssh	4.7	All	All	All
Application	Openbsd	Openssh	4.7p1	All	All	All
Application	Openbsd	Openssh	4.8	All	All	All
Application	Openbsd	Openssh	4.9	All	All	All
Application	Openbsd	Openssh	5.0	All	All	All
Application	Openbsd	Openssh	5.1	All	All	All
Application	Openbsd	Openssh	5.2	All	All	All
Application	Openbsd	Openssh	5.3	All	All	All
Application	Openbsd	Openssh	5.4	All	All	All
Application	Openbsd	Openssh	5.5	All	All	All
Application	Openbsd	Openssh	All	All	All	All

cpe:2.3:a:openbsd:openssh:1.2:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:1.2.1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:1.2.2:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:1.2.27:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:1.2.3:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:1.3:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:4.5:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:1.5:*****:

cpe:2.3:a:openbsd:openssh:1.5.7:*****:

cpe:2.3:a:openbsd:openssh:1.5.8:*****:

cpe:2.3:a:openbsd:openssh:2.1:*****:

cpe:2.3:a:openbsd:openssh:2.1.1:*****:

cpe:2.3:a:openbsd:openssh:2.2:*****:

cpe:2.3:a:openbsd:openssh:2.3:*****:

cpe:2.3:a:openbsd:openssh:2.3.1:*****:

cpe:2.3:a:openbsd:openssh:2.5:*****:

cpe:2.3:a:openbsd:openssh:2.5.1:*****:

cpe:2.3:a:openbsd:openssh:2.5.2:*****:

cpe:2.3:a:openbsd:openssh:2.9:*****:

cpe:2.3:a:openbsd:openssh:2.9.9:*****:

cpe:2.3:a:openbsd:openssh:2.9.9p2:*****:

cpe:2.3:a:openbsd:openssh:2.9p1:*****:

cpe:2.3:a:openbsd:openssh:2.9p2:*****:

cpe:2.3:a:openbsd:openssh:3.0:*****:

cpe:2.3:a:openbsd:openssh:3.0.1:*****:

cpe:2.3:a:openbsd:openssh:3.0.1p1:*****:

cpe:2.3:a:openbsd:openssh:3.0.2:*****:

cpe:2.3:a:openbsd:openssh:3.0.2p1:*****:

cpe:2.3:a:openbsd:openssh:3.0p1:*****:

cpe:2.3:a:openbsd:openssh:3.1:*****:

cpe:2.3:a:openbsd:openssh:3.1p1:*****:

cpe:2.3:a:openbsd:openssh:3.2:*****:

cpe:2.3:a:openbsd:openssh:3.2.2:*****:

cpe:2.3:a:openbsd:openssh:3.2.2p1:*****:

cpe:2.3:a:openbsd:openssh:3.2.3p1:*****:

cpe:2.3:a:openbsd:openssh:3.3:*****:

cpe:2.3:a:openbsd:openssh:4.4:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:4.4p1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:4.5:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:4.6:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:4.7:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:4.7p1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:4.8:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:4.9:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:5.0:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:5.1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:5.2:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:5.3:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:5.4:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:5.5:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:1.2:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:1.2.1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:1.2.2:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:1.2.27:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:1.2.3:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:1.3:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:1.5:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:1.5.7:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:1.5.8:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:2.1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:2.1.1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:2.2:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:2.3:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:2.3.1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:2.5:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:2.5.1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:2.5.2:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:2.9:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:2.9.9:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:2.9.9p2:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:2.9p1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:2.9p2:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.0:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.0.1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.0.1p1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.0.2:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.0.2p1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.0p1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.1p1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.2:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.2.2:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.2.2p1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.2.3p1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.3:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.3p1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.4:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.4p1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.5:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.5p1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.6:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.6.1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.6.1p1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.6.1p2:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.7:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.7.1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.7.1p1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.7.1p2:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.8:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.8.1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.8.1p1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.9:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.9.1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.9.1p1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:4.0:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:4.0p1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:4.1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:4.1p1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:4.2:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:4.2p1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:4.3:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:4.3p1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:4.3p2:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:4.4:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:4.4p1:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:4.5:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:4.6:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:4.7:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:4.7p1:*:*:*:*:*:


cpe:2.3:a:openbsd:openssh:4.8:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:4.9:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:5.0:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:5.1:*:*:*:*:*:
cpe:2.3:a:openbsd:openssh:5.2:*:*:*:*:*:
cpe:2.3:a:openbsd:openssh:5.3:*:*:*:*:*:
cpe:2.3:a:openbsd:openssh:5.4:*:*:*:*:*:
cpe:2.3:a:openbsd:openssh:5.5:*:*:*:*:*:
cpe:2.3:a:openbsd:openssh:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
 /r/ciscoUC	Several high vulnerabilities reported in CUCM OpenSSH. How do I resolve?	2022-05-31 16:31:04

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)