



CVE-2020-5591

Published on: 06/05/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:03 PM UTC

CVE-2020-5591

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Xack Dns](#) from [Xack](#) contain the following vulnerability:

XACK DNS 1.11.0 to 1.11.4, 1.10.0 to 1.10.8, 1.8.0 to 1.8.23, 1.7.0 to 1.7.18, and versions before 1.7.0 allow remote attackers to cause a denial of service condition resulting in degradation of the recursive resolver's performance or compromising the recursive resolver as a reflector in a reflection attack.

CVE-2020-5591 has been assigned by [vultures@jpcert.or.jp](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [XACK, Inc.](#) - **XACK DNS** version 1.11.0 to 1.11.4, 1.10.0 to 1.10.8, 1.8.0 to 1.8.23, 1.7.0 to 1.7.18, and versions before 1.7.0

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
-------------	------	------

No Description Provided

Vendor Advisory

xack.co.jp

text/html

MISC xack.co.jp/info/?ID=622

JVN#40208370: XACK DNS vulnerable to denial-of-service (DoS)

Mitigation

Third Party Advisory

VDB Entry

jvn.jp

text/xml

MISC jvn.jp/en/jp/JVN40208370/index.html

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	Xack	Xack Dns	All	All	All	All
Application	Xack	Xack Dns	All	All	All	All
Application	Xack	Xack Dns	All	All	All	All
Application	Xack	Xack Dns	All	All	All	All

cpe:2.3:a:xack:xack_dns:*****:

cpe:2.3:a:xack:xack_dns:*****:

cpe:2.3:a:xack:xack_dns:*****:

cpe:2.3:a:xack:xack_dns:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→