DoS via `op_response` packet from client

High **dyemanov** published **GHSA-7jq3-6j3c-5cm2** 7 hours ago

Package

No package listed

Affected versions

>=3

Patched versions

6.0, 5.0.4, 4.0.7, 3.0.14

Description

Summary

Incorrect decoding of the 'op_response' packet can cause a crash when parsing the status vector.

Details

The main problem is inside `xdr_status_vector()`, it doesn't handle `isc_arg_cstring` at all, so if an `isc_arg_cstring` is contained in the status vector, incorrect parsing will cause the server to crash. Basically there is no reason to send `op_response` from the client, the request will be dropped later in `loopThread()`, but the server should not fail anyway.

▶ Stacktrace

PoC

To reproduce the vulnerability, simply run the server and the Python script to emulate the malicious packet.

▶ Python script

Impact

Essentially, every server is affected.

Affected versions

Tested on v5 and v6, but code looks old, so it possible that v4 and v3 also affected.

Severity

High 7.5 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	None
Availability	High

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE ID

CVE-2026-34232

Weaknesses

No CWEs