Buffer overflow on parsing corrupted slice packet

High **dyemanov** published **GHSA-89mq-229g-x47p** 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

An unsafe deserialization of slice packet allows any unauthenticated user to perform a buffer overflow attack, which could lead to server crash or security vulnerabilities.

Details

The main bug is in `bool_t xdr_datum(xdr_t* xdrs, const dsc* desc, UCHAR* buffer)` when `desc` is a cstring. When parsing a cstring, compliance with the slice descriptor is not checked, i.e., if the length of the cstring exceeds the length of the descriptor (or the length of the entire slice), this cstring will be written to a buffer whose length is equal to the length of the slice, which will lead to a buffer overflow.

▶ Stacktrace when a program crashes due to buffer overflow

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.

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-2026-33337

Weaknesses

No CWEs