Pre-authentication out-of-bounds reads in dynamic channel parser in xrdp

High **metalefty** published **GHSA-92mr-6wpp-27jj** 5 hours ago

Package

No package listed

Affected versions

< 0.10.6

Patched versions

0.10.6

Description

Summary

xrdp through 0.10.5 has an out-of-bounds read vulnerability in pre-authentication RDP message parsing logic. A remote, unauthenticated attacker can trigger this flaw by sending a specially crafted sequence of packets during the initial connection phase. This vulnerability results from insufficient validation of input buffer lengths before processing dynamic channel communication. Successful exploitation can lead to a denial-of-service (DoS) condition via a process crash or potential disclosure of sensitive information from the service's memory space.

Severity

High 8.8 / 10

CVSS v4 base metrics

Exploitability Metrics

Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User interaction	None

Vulnerable System Impact Metrics	
Confidentiality	Low
Integrity	None
Availability	High
Subsequent System Impact Metrics	
Confidentiality	None
Integrity	None
Availability	None

Learn more about base metrics

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:H/SC:N/SI:N/SA:N

CVE ID

CVE-2026-33689

Weaknesses

▶ CWE-125