Pre-authentication out-of-bounds reads in RDP capability in xrdp

High **metalefty** published **GHSA-rvh9-9wm3-28c7** 5 hours ago

Package

No package listed

Affected versions

< 0.10.6

Patched versions

0.10.6

Description

Summary

xrdp through version 0.10.5 contains an out-of-bounds read vulnerability during the RDP capability exchange phase. The issue occurs when memory is accessed before validating the remaining buffer length. A remote, unauthenticated attacker can trigger this vulnerability by sending a specially crafted Confirm Active PDU. Successful exploitation could lead to a denial of service (process crash) or potential disclosure of sensitive information from the process memory.

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-2026-33516

Weaknesses

▶ CWE-125

Credits

exploitintel Reporter