Heap buffer overflow in NeutrinoRDP channel reassembly in xrdp

High **metalefty** published **GHSA-phw3-qp59-x2v4** 5 days ago

Package

No package listed

Affected versions

<= 0.10.1

Patched versions

0.10.6

Description

Summary

xrdp through version 0.10.5 contains a heap-based buffer overflow vulnerability in the NeutrinoRDP module. When proxying RDP sessions from xrdp to another server, the module fails to properly validate the size of reassembled fragmented virtual channel data against its allocated memory buffer. A malicious downstream RDP server (or an attacker capable of performing a Man-in-the-Middle attack) could exploit this flaw to cause memory corruption, potentially leading to a Denial of Service (DoS) or Remote Code Execution (RCE).

The NeutrinoRDP module is not built by default. This vulnerability only affects environments where the module has been explicitly compiled and enabled. Users can verify if the module is built by checking for `--enable-neutrinordp` in the output of the `xrdp -v` command.

Severity

High 7.7 / 10

CVSS v4 base metrics

Exploitability Metrics

Attack Vector	Network
Attack Complexity	Low

Attack Requirements	Present
Privileges Required	None
User interaction	Passive
Vulnerable System Impact Metrics	
Confidentiality	High
Integrity	High
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:P/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CVE ID

CVE-2026-32623

Weaknesses

▶ CWE-122

Credits

exploitintel Reporter