

# Heap buffer overflow in xrdp

**Moderate** metalefty published **GHSA-7q2g-6fjr-h6pp** 5 days ago

## Package

No package listed

## Affected versions

< 0.10.6

## Patched versions

0.10.6

## Description

### Summary

xrdp through version 0.10.5 contains a heap-based buffer overflow vulnerability in its logon processing. In environments where `domain_user_separator` is configured in `xrdp.ini`, an unauthenticated remote attacker can send a crafted, excessively long username and domain name to overflow the internal buffer. This can corrupt adjacent memory regions, potentially leading to a Denial of Service (DoS) or unexpected behavior.

The `domain_name_separator` directive is commented out by default, systems are not affected by this vulnerability unless it is intentionally configured.

## Severity

**Moderate** 6.3 / 10

### CVSS v4 base metrics

#### Exploitability Metrics

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

**Vulnerable System Impact Metrics**

Confidentiality	None
Integrity	Low
Availability	Low

**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:N/VC:N/VI:L/VA:L/SC:N/SI:N/SA:N

**CVE ID**

CVE-2026-32624

**Weaknesses**

▶ CWE-122

**Credits**

 exploitintel

Reporter