مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Remote Code Execution Vulnerability in xrdp

Tracking #:432318920

Date:08-05-2026



**TLP: WHITE**

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical remote code execution (RCE) vulnerability, identified as CVE-2025-68670, has been disclosed in the xrdp service.

## TECHNICAL DETAILS:

A critical remote code execution (RCE) vulnerability, identified as CVE-2025-68670, has been disclosed in the xrdp service. The vulnerability arises from improper bounds checking when processing user-supplied domain information during the Remote Desktop Protocol (RDP) connection sequence. Successful exploitation may allow unauthenticated remote attackers to execute arbitrary code on vulnerable systems without requiring user interaction.

**Vulnerability Details:**

- **CVE ID:** CVE-2025-68670
- **CVSS v3 Base Score:** 9.1, Critical
- **Affected Software:** xrdp
- **Issue Type:** Remote Code Execution (RCE) / Stack-based Buffer Overflow
- **CWE:** CWE-121
- **Attack Vector:** Network
- **Privileges Required:** None
- **User Interaction:** None
- **Impact:** Arbitrary code execution, service crash, memory corruption
- **Root Cause:** Improper bounds checking of domain string length during RDP connection processing
- **Affected Versions:** xrdp versions earlier than 0.10.5
- **Patched Versions:** 0.10.5
- **Exploitation Complexity:** Low
- **Exploitation Requirements:** Specially crafted RDP connection request
- **Potential Risk:** Remote attackers may overwrite stack memory and redirect execution flow

## RECOMMENDATIONS:

- Upgrade xrdp Immediately to fixed version.
- Avoid exposing RDP services directly to the internet.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

## REFERENCES:

- https://github.com/neutrinolabs/xrdp/security/advisories/GHSA-rwvg-gp87-gh6f