Insecure default and unsanitised AlternateShell handling in xrdp enables authenticated remote command execution

Moderate **metalefty** published **GHSA-rmvv-7633-fg7h** 5 hours ago

Package

xrdp

Affected versions

< 0.10.6

Patched versions

0.10.6

Description

Summary

xrdp through version 0.10.5 allows an authenticated remote user to execute arbitrary commands on the server due to unsafe handling of the AlternateShell parameter in xrdp-sesman.

When the `AllowAlternateShell` setting is enabled (which is the default when not explicitly configured), xrdp accepts a client-supplied AlternateShell value and executes it via `/bin/sh -c` during session initialization. This results in shell-interpreted execution of unsanitised, user-controlled input.

This behaviour effectively provides a scriptable remote command execution primitive over RDP within the security context of the authenticated user, occurring prior to normal window manager startup. This can bypass expected session initialization flows and operational assumptions that restrict execution to interactive desktop environments.

Severity

Moderate 6.3 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity	Low
Availability	Low

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L

CVE ID

CVE-2026-33145

Weaknesses

No CWEs

Credits

smittix Reporter