Heap overflow in dynvc processing in xrdp

High **metalefty** published **GHSA-jg6p-7fg8-9hh6** 5 hours ago

Package

xrdp

Affected versions

< 0.10.6

Patched versions

0.10.6

Description

Summary

xrdp through 0.10.5 has a heap-based buffer overflow vulnerability in its implementation of EGFX channel. This issue arises from the lack of proper validation for client-controlled size parameters during data processing on the graphics dynamic virtual channel. A remote attacker could exploit this flaw by sending specially crafted PDUs to trigger an out-of-bounds write, potentially leading to a denial of service (system crash) or arbitrary code execution (RCE). While the vulnerability is reachable both pre-authentication and post-authentication, pre-auth exploitation is primarily limited to causing a process crash, whereas achieving remote code execution typically requires hijacking specific processes that occur after successful user authentication.

Mitigation

The ultimate impact of this vulnerability depends heavily on the privileges under which the xrdp daemon is operating. Starting with version 0.10.2, xrdp officially introduced the capability to run the daemon as a non-privileged user rather than root. Many modern Linux distributions now implement this non-privileged execution as the default configuration. In such environments, even if an attacker successfully executes arbitrary code, their access is restricted to the limited service account, significantly hindering their ability to gain full administrative control (root access) over the entire operating system.

If an immediate upgrade to a patched version is not feasible, ensure that the xrdp daemon is configured to execute as a non-privileged user. Please refer to the `runtime_user` and `runtime_group` description in the `xrdp.ini(5)` man page for the unprivileged xrdp daemon configuration.

Severity

High 8.7 / 10

CVSS v4 base metrics

Exploitability Metrics	
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	Low
User interaction	None
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:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CVE ID

CVE-2026-35512

Weaknesses

▶ CWE-122

Credits

hessandrew Reporter