Undetected RDP traffic modification due to missing MAC verification in xrdp

Critical **metalefty** published **GHSA-j2jm-c596-c5q3** 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 does not implement verification for the Message Authentication Code (MAC) signature of encrypted RDP packets when using the "Classic RDP Security" layer. While the sender correctly generates signatures, the receiving logic lacks the necessary implementation to validate the 8-byte integrity signature, causing it to be silently ignored. An unauthenticated attacker with man-in-the-middle (MITM) capabilities can exploit this missing check to modify encrypted traffic in transit without detection.

It does not affect connections where the TLS security layer is enforced.

Mitigation

Users are advised to upgrade to a patched version. Otherwise, configure `xrdp.ini` to enforce TLS security (`security_layer=tls`) to ensure end-to-end integrity.

Severity

Critical 9.3 / 10

CVSS v4 base metrics

Exploitability Metrics

Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User interaction	None
Vulnerable System Impact Metrics	
Confidentiality	None
Integrity	High
Availability	Low
Subsequent System Impact Metrics	
Confidentiality	High
Integrity	High
Availability	Low

Learn more about base metrics

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:H/VA:L/SC:H/SI:H/SA:L

CVE ID

CVE-2026-32105

Weaknesses

▶ CWE-354

Credits

exploitintel Reporter