NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-66402

Summary

CVE-2026-66402 is a newly disclosed Critical vulnerability. It is not yet on CISA's actively-exploited list; treat it as proactive patching before it is weaponised. FreeRDP before 3.29.0 (affected versions <= 3.28.0) contains multiple TLS certificate identity validation weaknesses in tls_verify_certificate(), tls_match_hostname(), and x509_utils_get_dns_names(). Because FreeRDP performs custom Common Name and DNS SAN string matching instead of using OpenSSL's length-aware identity validation APIs, it (1) truncates DNS SAN values at embedded NUL bytes (accepting e.g. 'victim.example\0.attacker.example' as 'victim.example'), (2) accepts a matching Common Name even when non-matching DNS SAN entries are present, and (3) accepts IP-literal targets via DNS/CN matching without comparing iPAddress SANs. Under a trusted or misissued certificate chain, an attacker positioned to present such a certificate can bypass server identity verification, weakening TLS server authentication.

What we know

- **CVE:** CVE-2026-66402
- **Status:** Newly disclosed, not yet known-exploited (not on CISA KEV)
- **Severity:** CVSS 9.8 Critical, Network-exploitable, no privileges required, no user interaction (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Recommended action

Patch as a fix becomes available, prioritised by the exposure and EPSS above. Until then, restrict network access to the affected service now (segment it, put it behind a VPN, or take it offline) until you can patch. This does not yet trigger CRA 24-hour reporting, which requires active exploitation, but patching ahead of exploitation is the whole point.

Sources: NIST NVD. Public data; an advisory of a newly disclosed vulnerability, not an incident report. Verify applicability to your estate before acting.