RC: 511485

Advisory: Security Risk on Open RDP Port

Summary

Our security monitoring has identified that Remote Desktop Protocol (RDP) services are enabled and publicly accessible on one or more client systems. Exposing RDP directly to the internet significantly increases the risk of unauthorized access, system compromise, and potential ransomware attacks. This advisory outlines the risk, possible consequences, and recommended mitigation measures.

Description

Remote Desktop Protocol (RDP) is a privileged administrative service designed to allow remote access and system management. When RDP ports (commonly TCP 3389) are exposed to the public internet without adequate controls, they become prime targets for automated scans, brute-force attacks, credential stuffing, and exploitation of known or zero-day vulnerabilities.

Threat actors frequently leverage exposed RDP services as an initial access vector, especially in environments lacking multi-factor authentication, network restrictions, or active monitoring. Even with strong credentials in place, publicly accessible RDP remains vulnerable due to persistent attack attempts and evolving exploit techniques.

Consequences

Leaving RDP ports open to the internet may result in:

a) Unauthorized system access through brute-force or credential-based attacks.
b) Exploitation of RDP or operating system vulnerabilities.
c) Privilege escalation and lateral movement across internal systems.
d) Deployment of ransomware, malware, or data exfiltration tools.
e) Service disruption, data loss, and reputational damage.
f) Non-compliance with regulatory requirements and internal security policies.

RC: 511485

Solution / Mitigation

To reduce this risk, customers are strongly advised to restrict or completely block RDP access from the public internet.

Recommended actions include:

a. Disable direct RDP access from the internet wherever possible.
b. Restrict RDP access to trusted internal networks or approved IP addresses only.
c. Enforce Multi-Factor Authentication (MFA) for all remote access.
d. Use secure remote access alternatives such as VPNs, bastion hosts, or remote access gateways.
e. Apply the latest security patches to operating systems and RDP-related services.
f. Implement account lockout policies and continuous monitoring for failed login attempts.
g. Periodically review firewall and network configurations to ensure RDP remains restricted.

Security Best Practice

As a general security principle, administrative services such as RDP should never be exposed to the public internet unless there is a clearly defined and justified business need, supported by strong compensating controls.