RC: 511485

Advisory: Security Risk on Open SSH Port

Summary

Our security monitoring has revealed that numerous client systems have Secure Shell (SSH) service running and accessible on the internet. The likelihood of illegal access and system breach is greatly increased by this misconfiguration. This advisory describes the problem, it's possible consequences, and some solutions.

Description

SSH is a privileged administrative service designed for secure system administration. When exposed publicly without strict access controls, it becomes a frequent target for automated attacks. Internet-wide scanners continuously probe for open SSH ports and attempt to exploit weak credentials, misconfigurations, or unpatched vulnerabilities.

Even when strong passwords are used, publicly accessible SSH services remain at risk due to persistent brute-force activity and evolving exploit techniques.

Consequences

Leaving SSH ports open to the internet may result in:

a. Unauthorized system access through brute-force or credential-stuffing attacks.
b. Exploitation of SSH or operating system vulnerabilities.
c. Privilege escalation and lateral movement within your environment.
d. Data exfiltration, service disruption, or malware deployment.
e. Violation of regulatory compliance requirements or internal security policies.

Solution / Mitigation

To reduce this risk, customers are strongly advised to block SSH access from the public internet.

Recommended actions include:

a. It is advisable to use SSH key instead of password.
b. Close or block SSH ports so they are not reachable from the internet.
c. Allow SSH access only when absolutely necessary, and only from trusted internal networks or approved locations.

d. Use secure alternatives such as private networks or controlled access gateways for remote administration.
e. Periodically review network settings to ensure SSH remains restricted.

As a general security principle, administrative access should never be publicly exposed unless there is a clear and justified business need.