Stakeholder Briefing

Author: Harshal Harekar
Date: 30/10/2025

Briefing

During our recent security assessment, we identified and exploited a critical vulnerability in the FTP service of a test system. Using industry-standard tools, we gained remote access through a known flaw in vsftpd version 2.3.4. Additionally, we tested the system's APIs and found weaknesses in input validation that could allow unauthorized access or data manipulation.

All vulnerabilities were responsibly disclosed and remediated. The FTP service was upgraded, and the APIs were hardened with proper validation and access controls. A follow-up scan confirmed that the issues were resolved.

This exercise highlights the importance of regular security testing, timely patching, and strong input validation. We recommend ongoing monitoring and periodic assessments to maintain a secure posture.