🔴Risk 1, involves a known vulnerability in phpMyAdmin (CVE-2005-3299) that allows Local File Inclusion (LFI). This flaw enables remote attackers to access sensitive server files such as `/etc/passwd`, potentially leading to further system compromise. The vulnerability is accessible via the web if phpMyAdmin is left unprotected. It is strongly recommended to immediately patch the affected components and restrict external access to phpMyAdmin, preferably through IP whitelisting or VPN.

🟠 Risk 2 concerns the FTP service running version 3.4.0r16, which does not support encrypted connections. This exposes the system to credential leakage or unauthorized access by network-based attackers. To mitigate this, organizations should disable FTP entirely or transition to SFTP, ensuring credentials are encrypted in transit and protected by strong authentication methods.

🟠 Risk 3 involves the F5 BIG-IP HTTP proxy in use, which may be improperly configured. This creates a possible attack vector for internal actors or man-in-the-middle (MitM) attacks, where traffic may be intercepted or redirected. To reduce this risk, it is advised to harden the proxy configuration and implement a Web Application Firewall (WAF) to filter malicious traffic and prevent exploitation.

🟢 Risk 4 highlights that the SMTP service on port 25 is filtered or unresponsive, which may point to a misconfiguration or unintended blocking by firewall rules. While this risk is relatively low, it is still important to review SMTP configurations and logs to ensure the service is operating securely and correctly within the intended communication scope.