Mitigation Plan for SSL Certificate Issues

Based on the SSL certificate issues identified during our asset scanning process, we recommend the following mitigation strategies to enhance your organization's security posture and maintain smooth operations.

1. **Implement Certificate Lifecycle Management**
   - Deploy an automated certificate management system to track expiration dates.
   - Set up alerts for certificates nearing expiration (e.g., 30, 14, and 7 days before expiry).
   - Automate the renewal process where possible to prevent unexpected expirations.
2. **Standardize on Strong Cryptography**
   - Use a minimum of 2048-bit RSA keys or 256-bit ECC keys for all certificates.
   - Employ SHA-256 or stronger for certificate signatures.
   - Phase out any remaining SHA-1 or MD5 based certificates immediately.
3. **Ensure Proper Hostname Matching**
   - Conduct regular audits to ensure all certificates match the hostnames they're served from.
   - Implement a review process for new certificate requests to verify correct domain names.
   - Use Subject Alternative Name (SAN) certificates for multi-domain coverage instead of wildcards where possible.
4. **Eliminate Self-Signed Certificates**
   - Replace all self-signed certificates on production and public-facing systems with CA-issued certificates.
   - If self-signed certificates are necessary for internal purposes, implement a proper internal CA infrastructure.
5. **Monitor Certificate Revocation**
   - Implement automated checking of Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP).
   - Establish a process for immediate replacement of revoked certificates.
6. **Upgrade SSL/TLS Protocols**
   - Disable SSL 2.0, SSL 3.0, TLS 1.0, and TLS 1.1 on all servers.
   - Configure servers to use TLS 1.2 or TLS 1.3 exclusively.
   - Regularly check for and apply security updates to SSL/TLS libraries (e.g., OpenSSL).
7. **Ensure Certificate Transparency Compliance**
   - Use only certificates that are logged in Certificate Transparency logs.
   - Implement CT monitoring to detect unauthorized certificate issuance for your domains.

8. **Limit and Secure Wildcard Certificates**
    - Restrict the use of wildcard certificates to specific, necessary cases.
    - Implement extra security measures for wildcard certificate private keys, such as hardware security modules (HSMs).
    - Consider splitting wildcard certificates into multiple specific certificates where feasible.
9. **Verify Complete Certificate Chains**
    - Ensure all intermediate certificates are properly installed on servers.
    - Regularly test certificate chain validity using online SSL checkers or internal tools.
10. **Enhance Private Key Security**
    - Store private keys in hardware security modules (HSMs) where possible.
    - Implement strict access controls and logging for systems with access to private keys.
    - Establish a process for immediate certificate replacement if key compromise is suspected.
11. **Regular Security Assessments**
    - Conduct periodic (e.g., quarterly) scans of all assets to identify SSL/TLS issues.
    - Perform annual penetration testing that includes assessment of SSL/TLS configurations.
12. **Establish a Certificate Policy**
    - Develop and enforce an organizational policy for certificate issuance, use, and management.
    - Include guidelines for approved CAs, key lengths, and certificate types.
13. **Employee Training and Awareness**
    - Provide training to IT staff on proper SSL/TLS configuration and certificate management.
    - Raise awareness among developers about the importance of proper certificate usage in applications.
14. **Incident Response Planning**
    - Include SSL/TLS-related scenarios in your incident response plan.
    - Conduct drills to practice rapid response to certificate compromises or unexpected expirations.
15. **Vendor Management**
    - Establish requirements for proper SSL/TLS usage in contracts with third-party service providers.
    - Regularly audit vendor compliance with these requirements.

By implementing these mitigation strategies, your organization can significantly reduce the risks associated with SSL certificate issues, enhance overall security, and ensure uninterrupted service for your users. Regular review and updating of these practices will help maintain a robust SSL/TLS security posture in the face of evolving threats and standards.

Revision #1
Created 19 September 2024 10:50:07 by Admin
Updated 19 September 2024 10:50:27 by Admin