ADVISORY FOR ICM SECTOR

Credential Management Guidelines

Original report published on: March 20, 2026

Executive Summary

Recent incidents across critical information infrastructure and enterprise environments have highlighted weaknesses in credential handling and operational hygiene that may introduce significant security vulnerabilities. These weaknesses can be exploited by threat actors to gain unauthorised access, escalate privileges, and maintain persistence within targeted environments.

These guidelines outline three key risk areas: unprotected credential storage, password reuse across accounts, and structured or predictable password patterns. Organisations are strongly encouraged to review and address these issues to reduce their exposure to credential-based attacks.

1) Unprotected Storage of Credentials

Scripts and configuration files used for system administration may contain sensitive authentication material, including credentials for privileged access to virtual machines, firewalls, network devices, and customer edge systems.

Insecure practices have been observed where such credentials are stored in cleartext on jump hosts or hard coded within configuration files and software code repositories, including API keys. This increases the risk of credential exposure and unauthorised use.

Organisations are advised to:

1. Conduct audits of all jump hosts and remove any stored credentials, authentication materials, or secrets.
2. Store credentials using approved cryptographic methods within credential or secrets management systems and enforce role-based access controls.
3. Implement Privileged Access Management (PAM) solutions, including credential vaulting, privileged session monitoring, and session isolation through gateways or proxies to prevent the exposure of privileged credentials and eliminate the need for local credential storage.
4. Where PAM solutions are deployed, configure automatic rotation of privileged credentials after each checkout or session, where supported.
5. Review software code repositories to identify and remove hard-coded credentials, including API keys, tokens, and other secrets.

2) Password Reuse Across Accounts

Reusing passwords across multiple accounts and environments can significantly increase the impact of credential compromise and facilitate lateral movement.

This risk is amplified when the same credentials are reused across different systems and environments, particularly between user and administrative accounts. A single compromised password may then be used to gain unauthorised access to multiple systems or services.

Organisations are advised to:

1. Educate users to avoid reusing passwords across all accounts, particularly between privileged and non-privileged accounts.
2. Implement password history controls to prevent the reuse of previously used passwords, including following password resets.
3. Enforce Multi-Factor Authentication (MFA) across all management interfaces, privileged accounts, and critical systems.
4. Monitor for compromised credentials using threat intelligence feeds and breached credential databases, and take appropriate remediation actions when compromised credentials are identified.

3) Structured or Predictable Passwords

Some passwords may follow predictable patterns, such as keyboard walks, sequential patterns, simple character substitutions, or passwords derived from organisation or system names. While these passwords may meet basic complexity requirements, they remain vulnerable to guessing attacks, password spraying, and brute-force attacks.

Organisations are advised to:

1. Implement controls to detect and reject structured or predictable passwords, including dictionary words, keyboard walks, sequential patterns, simple character substitutions, and passwords derived from organisation or system names.
2. Maintain and enforce blocklists of commonly used and previously breached passwords.
3. Enforce a minimum password length of 14 characters, or 8 characters where MFA or hardware-based authentication is implemented.
4. Conduct periodic password strength assessments across environments to identify weak credentials.
5. Implement password rotation policies requiring passwords for privileged or high-risk accounts to be rotated at least every 90 days, unless MFA or hardware-based authentication is implemented.