Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India

CERT-In Advisory CIAD-2022-0026

Password Management and Security

Original Issue Date: October 18, 2022

Description

Passwords are fundamental element of information security. They are used as a first-line defense in securing almost all electronic information, networks, servers, devices, accounts, databases, files, and more. A password policy is a set of rules to define, control and manage user passwords.

Majority of unauthorised access incidents, credentials leak, data breaches are caused due to poor password management policies by organizations. Password management is a combination of strong password policies and Multi-Factor Authentication (MFA) to reduce the harm that could be caused by phishing, credentials leak or unauthorized access attacks.

Effective password management facilitates IT/security teams to maintain password hygiene and create unique passwords easily. Password protection is one of several primary safeguards to restrict access to the network and data within it.

The following best practices are recommended for using improving the password management and security.

- Create awareness among all staff of organization on importance of maintaining secure passwords.
- Use Strong Passwords. A Strong Password should:
    - Be of at least 8 characters in length
    - Contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z)
    - Have at least one numerical character (e.g. 0-9)
    - Have at least one special character (e.g. ~!@#$%^&*()_-+=)
- Systems should be designed to accept and transmit passwords with proper safeguards such as
    - Passwords should not be displayed while entered and also should not be saved in web browsers
    - Passwords should not be stored in clear text or in automated login script
    - Passwords must be secured with Multifactor authentication (MFA).
    - Password hashes must be protected
    - Use pass phrases for encryption
- An effective password management or password vault solution may be used within organisation, and made available for all staff.
- Utilise password management solutions or password vault solutions to set policies to auto-generate long & unique passwords and to periodically change passwords.

Required Security features for Password management

- Cloud-based options can be more flexible to access from wherever you need, easier to set up and easier to maintain. However, it does require trusting the provider and ensure that the solution is hosted within India.
- Locally hosted options require less trust in external parties, but requires ongoing maintenance. It may limit your ability to access from external locations such as staff working remotely. Cloud or locally hosted solutions may be chosen according to organization’s need.
- The password management solutions should have up-to-date encryption algorithms with multiple layers of encryption.
- Strong encryption key practices are also important in the cases of cloud-based password management solutions.
- Multi-factor authentication should be used for accessing the password database and resetting master password, especially if the password management solution is cloud-based.
- Secure and safe provisions should be used for sharing Shared passwords with authorized people.
- Logging information features should be used to see every time a user views or copies a password for traceability.
- The password management solutions should have features to generate passwords or passphrases, which can be set to generate minimum or maximum length passwords.

References

https://www.cisa.gov/mfa
https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/authentication-methods
https://www.cmu.edu/iso/governance/guidance/password-managers.html

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-24368572

Postal address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India