Unsecured Credentials, Technique T1552 - Enterprise

Archived: 2026-04-05 15:40:45 UTC

ID	Mitigation	Description
M1015	Active Directory Configuration	Remove vulnerable Group Policy Preferences.[8]
M1047	Audit	Preemptively search for files containing passwords or other credentials and take actions to reduce the exposure risk when found.
M1041	Encrypt Sensitive Information	When possible, store keys on separate cryptographic hardware instead of on the local system.
M1037	Filter Network Traffic	Limit access to the Instance Metadata API. A properly configured Web Application Firewall (WAF) may help prevent external adversaries from exploiting Server-side Request Forgery (SSRF) attacks that allow access to the Cloud Instance Metadata API.[9]
M1035	Limit Access to Resource Over Network	Limit network access to sensitive services, such as the Instance Metadata API.
M1028	Operating System Configuration	There are multiple methods of preventing a user's command history from being flushed to their .bash_history file, including use of the following commands: `set +o history` and `set -o history` to start logging again; `unset HISTFILE` being added to a user's .bash_rc file; and `ln -s /dev/null ~/.bash_history` to write commands to `/dev/null` instead.
M1027	Password Policies	Use strong passphrases for private keys to make cracking difficult. Do not store credentials within the Registry. Establish an organizational policy that prohibits password storage in files.

ID	Mitigation	Description
M1026	Privileged Account Management	If it is necessary that software must store credentials in the Registry, then ensure the associated accounts have limited permissions so they cannot be abused if obtained by an adversary.
M1022	Restrict File and Directory Permissions	Restrict file shares to specific directories with access only to necessary users.
M1051	Update Software	Apply patch KB2962486 which prevents credentials from being stored in GPPs.[10][11]
M1017	User Training	Ensure that developers and system administrators are aware of the risk associated with having plaintext passwords in software configuration files that may be left on endpoint systems or servers.

ID	Name	Analytic ID	Analytic Description
DET0412	Detect Access or Search for Unsecured Credentials Across Platforms	AN1153	Unusual access to bash history, registry credentials paths, or private key files by unauthorized or scripting tools, with correlated file and process activity.
		AN1154	Reading of sensitive files like .bash_history, /etc/shadow, or private key directories by unauthorized users or unusual processes.
		AN1155	Unusual access to ~/Library/Keychains, ~/.bash_history, or Terminal command history by unauthorized processes or users.
		AN1156	Unusual web-based access or API scraping of password managers, single sign-on sessions, or credential sync services via browser automation or anomalous API tokens.

ID	Name	Analytic ID	Analytic Description
		AN1157	Unauthorized API or console calls to retrieve or reset password credentials, download key material, or modify SSO settings.
		AN1158	Access to container image layers or mounted secrets (e.g., Docker secrets) by processes not tied to entrypoint or orchestration context.
		AN1159	Use of configuration backup utilities or CLI access to dump plaintext passwords, local user hashes, or SNMP strings.
