Credentials in Files (version 1.1)

**Cloud Service Label: IaaS, PaaS**

Description

Adversaries may search local file systems and remote file shares or registries for files containing passwords. These can be files created by users to store their own credentials, shared credential stores for a group of individuals, configuration files containing passwords for a system or service, or source code/binary files containing embedded passwords. It is possible to extract passwords from backups or saved virtual machines through Credential Dumping.

In cloud environments, authenticated user credentials are often stored in local configuration and credential files. Developers may also embed cloud resource credentials in code to streamline the access of data from a database or file store believing the content all traffic will be contained within the cloud. In some cases, these credentials can be collected and reused on another machine or the contents can be read and then used to authenticate without needing to copy any files. In some scenarios adversaries can use credentials found in files to perform lateral movement.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| CVE-2019-1003062 | Jenkins AWS CloudWatch Logs Publisher Plugin stores credentials unencrypted in job config.xml files on the Jenkins master. These credentials can be viewed by users with Extended Read permission, or access to the master file system. |

Mitigations

|  |  |  |
| --- | --- | --- |
| **Mitigation** | | **Description** |
| Audit | | Frequently check permissions on cloud storage to ensure proper permissions are set to deny open or unprivileged access to resources. Consider using automated resource checkers such as CloudSploit or Divvycloud. |
|  | *AWS* | To perform an audit via AWS it is suggested to review information such as account details (credentials, users, groups, roles, etc), mobile applications, EC2 configurations, policies, and account activity. How to audit these different factors can be found in detail at: **https://docs.aws.amazon.com/general/latest/gr/aws-security-audit-guide.html.** |
|  | *Azure* | To perform an audit via Azure an administrator can review the audit logs that are recorded under Azure’s monitoring for active directory. The audit logs allow for filtering, as well as looking at users, groups, and enterprise specific information. Full details on how to access this information can be found at: **https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-audit-logs.** |
|  | *GCP* | To perform an audit via GCP the logs can be reviewed. GCP breaks this down into three categories; admin activity, data access, and system events. The audit logs can be viewed a few different ways- the console, API, or gcloud. Full details on how to view these logs, how to export, and for how to configure the retention period can be found here: **https://cloud.google.com/logging/docs/audit.** |
| Password Policies | | Establish an organizational policy that requires good password practices. This includes that passwords are never stored in plaintext. |
|  | *AWS* | Good password practices can be enforced in AWS via the console, AWS CLI, and AWS API. These configurations are for IAM accounts only and have a range of different characteristics that can be enforced. For instance minimum password length, require a range of characters (lowercase, uppercase, number, and non alphanumeric ), allow users to change their own password, password expiration, prevent password reuse, and require administrator reset after password expiration. All details on how to configure these enforcement policies with all three management systems can be found here: [**https://docs.aws.amazon.com/IAM/latest/UserGuide/id\_credentials\_passwords\_account-policy.html**](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html)**.** |
|  | *Azure* | Good password practices can be enforced in Azure with Azure Active Directory using the resource manager deployment. By default these accounts have some policies enforced including amount of lockout duration, and allowed number of logon attempts. Other policies that can be changed are minimum password length and the ability to enforce the concept of ‘passwords complexity requirements’. These configurations can be accomplished by accessing the Active Directory Administrative Center under administrative tools, then editing the rules under the settings for the Password Settings Container. Full details on how to accomplish this can be found here:[**https://docs.microsoft.com/en-us/azure/active-directory-domain-services/password-policy**](https://docs.microsoft.com/en-us/azure/active-directory-domain-services/password-policy) |
| [Restrict File and Directory Permissions](https://attack.mitre.org/mitigations/M1022) | | Users should have limited access to files and directories depending on their need for access. The file and directory permissions should be restricted on the basis of least privilege. |
|  | *AWS* | To manage the files and directory permissions in AWS, IAM policies can be used. This can be done by utilizing group policies and policy variables. The policy would be created specifying the folder, then the permissions attached to that folder (whether the user has access to list out the objects within the directory, if they have read permissions, if they have write permissions, etc.), lastly the group that it applies to would be specified. The users can that be added and removed from that group as needed. Full details on how this can be done is explained here: **https://aws.amazon.com/blogs/security/writing-iam-policies-grant-access-to-user-specific-folders-in-an-amazon-s3-bucket/.** |
|  | *Azure* | To manage the files and directory permissions in an Azure environment basic and advanced system defined controls. This will be dependent on the type of system being used (Windows, Linux, etc). The permissions will be set individually or by group using the system commands or controls needed.. Full details on how this can be done is explained here: **https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-ad-ds-configure-permissions.** |
| Use Metadata Service | | Applications can use the metadata service accessible on the local interface to obtain  application tokens to access cloud resources. In Azure for example  GET '<http://169.254.169.254/metadata/identity/oauth2/token?api-version=2018-02-01>  &resource=https://management.azure.com/' HTTP/1.1 Metadata: true |
| [User Training](https://attack.mitre.org/mitigations/M1017) | | Ensure that developers and system administrators are aware of the risk associated with having plaintext passwords in software files that may be on endpoint systems or servers. |

Detection

While detecting adversaries accessing these files may be difficult without knowing they exist in the first place, it may be possible to detect adversary use of credentials and the suspicious activities they undertake with them. Consumers may also wish to monitor the command-line arguments of executing processes for suspicious words or regular expressions that may indicate searching for a password (for example: password, pwd, login, secure, or credentials). Audit application code for embedded passwords or keys.

|  |  |
| --- | --- |
| **Detection of activities after exploit** | **Description** |
| Create Log Metric Filters and Alarms for AWS | To create a metric filter and alarm:   1. Create a metric filter that checks for IAM policy changes and the *<cloudtrail\_log\_group\_name>* 2. Create an SNS topic 3. Create an SNS subscription to the above topic 4. Create an alarm associated with the filter and SNS topic created in steps 1 and 2 respectively |
| Monitor Activity in AWS Account | Various services in AWS offer logging features that allow for detection capabilities. These include CloudFront, CloudTrail, CloudWatch, Config, and S3. |
| Monitor for Suspicious Activity in Azure | Azure AD can generate anomaly reports than can be run on a daily basis. Azure AD Identity Protection show current risks in its dashboard and provides daily email summary notifications. Policies can also be configured to alert to specific issues. |
| Create Log Metric Filters and Alarms for CloudTrail | To create a metric filter and alarm:   1. Create a filter that checks for CloudTrail changes and the specific *<cloudtrail\_log\_group\_name>* 2. Create an SNS topic that the alarm will notify 3. Create an SNS subscription to the above topic 4. Create an alarm associated with the filter from step 1 and SNS topic in step 2 |
| Create Activity Log Alerts in Azure | To create log activity alerts for deletion in the Azure Console:   1. Navigate to *Monitor’ / ‘Alerts* 2. Select *Manage alert rules* 3. Click on the Alert *Name* where Condition contains *operationName equals Microsoft.Network/networkSecurityGroups/securityRules/delete* 4. Hover a mouse over *Condition* to ensure it is set to *Whenever the Administrative Activity Log “Delete Security Rule (networkSecurityGroups/securityRules)” has “any” level with “any” status and event is initiated by “any*” |
| Create, View, and Manage Activity Alerts in Azure Monitor | To create a log alert in the Azure portal:   1. Select **Monitor -> Alerts** 2. Select **New alert rule** of the **Alerts** window 3. Provide information in **Define alert condition** 4. Provide details in **Define alert details** 5. Specify action group for new alert rule under **Action group**, or create a new action group with + **New group** 6. Select **Yes** for the **Enable rule upon creation** option 7. Select **Create alert rule**   To view and manage alerts:   1. Select **Monitor -> Alerts -> Manage alert rules** 2. Select the rule you want to modify and double-click to edit the rule options 3. Click **Save** |
| Azure Resource Manager Templates | Azure Resource Manager templates in the format of JSON files that can be used to configure metric alerts in Azure Monitor. These templates can be used for simple static and dynamic threshold metric alerts, availability tests, and monitoring multiple resources. |
| Enable CloudTrail across all regions in AWS | To enable CloudTrail across all regions:   1. Sign into the AWS Management Console and open the CloudTrail console 2. Click on *Trails* 3. Set necessary Trails to All option in the I column 4. Click on a trail via the link *Name* column 5. Set *Logging* to *ON* 6. Set *Apply trail to all regions* to *Yes* |
| Configure log profile to capture activity logs for all regions in Azure | To set up activity logs for all regions:   1. Navigate to Azure console 2. Go to *Activity log* 3. Select *Export* 4. Select *Subscription* 5. Check *Select all* in *Regions* 6. Select *Save* |

References

1. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1003062. Retrieved June 7, 2020.