Insertion of Sensitive Information into Log File (combined with Collection from Cloud Logs)

(version 1.0)

**Cloud Service Label: IaaS**

Description

Adversaries may be able to use the cloud’s extensive logging capabilities, and the information written to them, as a way to gain information/access to a system. Ultimately, this can lead to the adversary gaining access to user data of a sensitive nature. Logging is essential for many aspects of day to day operations but logging of all information is not always necessary once a system is in production. Some types of log files that can be utilized are server log files, debugging logs, plugin logs, etc.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| CVE-2020-7599 | Adversaries may exploit a vulnerability in com.gradle.plugin-publish versions prior to 0.11.0 where an author publishes a plugin where the build log is public and the –info flag is used. Under these circumstances the build log will contain an AWS pre-signed URL that would allow an adversary to access the pre-signed URL, of a plugin that was recently uploaded, and replace it with their own plugin. |
| CVE-2019-4284 | IBM Cloud Private versions 2.1.0, 3.1.0, 3.1.1, and 3.1.2 contain a vulnerability that allows a local privileged user to view OpenID Connect tokens that could be printed to log files. These tokens could be utilized to log into the system as other users. |

Mitigations

|  |  |
| --- | --- |
| **Mitigation** | **Description** |
| Log Configurations | Make the decision on what is necessary to be logged and what is not. |
| Log File Permissions | Make sure that log files have permissions in place to avoid unauthorized read/write access. |
| AWS CIS Benchmark Standards | Refer to the logging section of the AWS CIS Benchmark Standards. These include ensuring CloudTrail is enabled in all regions, enabling log file validation, removing public access to S3 buckets, encrypting CloudTrail logs at rest using KMS CMKs, and enabling VPC flow logging in all VPCs, and integrating CloudTrail trails with CloudWatch Logs. |
| AWS CloudWatch Logs Documentation | IAM Identities (identity-based policies) can be attached to specific writing permissions policies. CloudWatch Log policies use AWS condition keys to express conditions. |
| Azure CIS Benchmark Standards | Refer to the logging section of the Azure CIS Benchmark Standards. These include ensuring that activity logs for storage containers are not publicly accessible and that they are encrypted with BYOK (Bring Your Own Key) |

Detection

|  |  |
| --- | --- |
| **Detection** | **Description** |
| Create Log Metric Filters and Alarms for CloudTrail to detect illicit logins and access | 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, View, and Manage Activity Alerts in Azure Monitor to detect illicit logins and access | 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** |

References

1. [CWE. (Feb 20, 2020). CWE-532: Insertion of Sensitive Information into Log File. Retrieved June 9, 2020.](https://cwe.mitre.org/data/definitions/532.html)
2. [CVE. (Jan 21, 2020). CVE-2020-7599. Retrieved June 9, 2020.](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7599)
3. <https://d0.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf>. Accessed July 27, 2020.
4. <https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/permissions-reference-cwl.html>. Accessed July 27. 2020.
5. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-4284>. Accessed August 6, 2020.
6. <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-activity-log>. Accessed August 6, 2020.
7. <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-metric-create-templates#template-for-a-metric-alert-that-monitors-multiple-resources>. Accessed August 6, 2020.