Sensitive Information Exposed on A Public Platform (version 1.0)

**Cloud Service Label: IaaS, PaaS, SaaS**

Description

Adversaries may be able to exploit information that is found exposed online. This type of information could include emails, usernames, passwords, keys, and any information considered sensitive that could be used to facilitate initial or prolonged access. Instances of this could include credentials uploaded to GitHub, information found on a server, or in numerous other places. Adversaries may be able to exploit sensitive information that is exposed. For this reason, configurations should be made to lock down any and all sensitive information and be vigilant when uploading information to publicly accessible resources. This can lead to initial access, privilege escalation, discovery, and collection.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| AWS Data Exposed on GitHub | An AWS engineer committed a gigabyte of data to a GitHub repository. This data included information such as access keys, authentication keys, API keys, and information listed as confidential. This data was a large amount and was accessible for five hours. |
| Google Dorking | Google Dorking is a technique utilizing specially crafted search queries to identify exposed credentials, vulnerable files, and system information on publicly hosted platform. Searching keywords like “aws”, “amazon”, “azure”, “microsoft cloud” will return results related to these cloud platforms. |

Mitigations

|  |  |
| --- | --- |
| **Mitigation** | **Description** |
| Sanitize Data | Always make sure to sanitize data before uploading to publicly accessible resources like the tool git-secrets. Git-secrets is a tool from AWSLabs’ GitHub meant to prevent a user from committing passwords and other sensitive information to a git repo. It is also used to scan a repository for already exposed credentials. |
| DLP Solutions | Data loss prevention software can prevent sensitive data from being exposed on a public platform by monitoring, detecting, and blocking an organization’s data. |

Detection

Monitor posts to public repositories for any sensitive information that can be exploited by an adversary. There are Cloud Access Security Brokers (CASB) that can be used to scan public repositories looking for an organization’s sensitive material, after the fact.

References

1. [Security Boulevard. (Jan 27, 2020). AWS Data Exposed on GitHub. Accessed June 10, 2020.](https://securityboulevard.com/2020/01/aws-data-exposed-on-github/)
2. <https://github.com/awslabs/git-secrets>. Accessed July 15, 2020.
3. <https://www.exploit-db.com/google-hacking-database>. Accessed July 15, 2020.