CloudTrail/Logging Exploits (version 1.0)

**Cloud Service Label: IaaS, PaaS**

Description

AWS CloudTrail and Azure Monitor logs are often parsed by people with increased rights or accesses. An attacker with limited access to a resource in an AWS/Azure account can craft a name for a request to the API that will certainly fail but will be logged by the cloud API logging service. If a cloud admin exports these logs for example to a spreadsheet in Excel or Google sheets, which is a common practice, the failed API request may actually contain a formula that will be executed inside a spreadsheet. This will probably be invisible to the admin who has now just unwittingly allowed one of several possible actions to be executed with his credentials.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Cloudtrail\_csv\_Injection | Open source Pacu module that automates CloudTrail attacks based on manipulation API calls. |

Mitigations

|  |  |
| --- | --- |
| **Mitigation** | **Description** |
| Review Logs Outside Spreadsheets | Don’t use spreadsheets to examine cloud-based logs. |

Detection

 This attack is nearly impossible to detect unless the administrator recognizes a crafted entry is present within cloud API logs before he attempts to examine it inside a spreadsheet.

References

1. https://www.we45.com/blog/2017/02/14/csv-injection-theres-devil-in-the-detail - Accessed 02/12/2020