System (VM) Information Discovery (version 1.1)

**Cloud Service Label: IaaS**

Description

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Windows | Example commands and utilities that obtain this information include ver, Systeminfo, and dir within cmd for identifying information based on present files and directories. |
| Application Discovery Service (AWS) | In Amazon Web Services (AWS), the Application Discovery Service may be used by an adversary to identify servers, virtual machines, software, and software dependencies running. |
| Google Cloud Platform (GCP) | GET /v1beta1/{{parent=organizations/}}/assets or  POST/v1beta1/{{parent=organizations/}}/assets:runDiscovery may be used to list an organizations cloud assets, or perform asset discovery on a cloud environment. |
| API Request (Azure) | In Azure, the API request GET [https://management.azure.com/subscriptions/{{subscriptionId}}/resourceGroups/{{resourceGroupName}}/providers/Microsoft.Compute/virtualMachines/{{vmName}}?api-version=2019-03-01](https://management.azure.com/subscriptions/%7b%7bsubscriptionId%7d%7d/resourceGroups/%7b%7bresourceGroupName%7d%7d/providers/Microsoft.Compute/virtualMachines/%7b%7bvmName%7d%7d?api-version=2019-03-01)  may be used to retrieve information about the model or instance view of a virtual machine. |
| Co-residence identification and Information Leakage detailed in academic papers | Specific information in hypervisors like privileged VM IP addresses and access keys used by machine admins can theoretically be inferred by occupying a VM on the same physical host as the target and performing clever cache queries to infer Information that normally would be protected by Cloud identity and access solutions. |

Mitigations

|  |  |
| --- | --- |
| **Mitigation** | **Description** |
|  | This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of cloud system features. |

Detection

Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through  [PowerShell](https://attack.mitre.org/techniques/T1086). And the CLI in cloud-based systems, native logging can be used to identify access to certain APIs and dashboards that may contain system information. Depending on how the environment is used, that data alone may not be useful due to benign use during normal operations.

References

1. [Amazon. (n.d.). What Is AWS Application Discovery Service?. Retrieved October 8, 2019.](https://docs.aws.amazon.com/en_pv/application-discovery/latest/userguide/what-is-appdiscovery.html)

1. [Google. (2019, October 3). Quickstart: Using the dashboard. Retrieved October 8, 2019.](https://cloud.google.com/security-command-center/docs/quickstart-scc-dashboard" \t "_blank)

1. [Microsoft. (2019, March 1). Virtual Machines - Get. Retrieved October 8, 2019.](https://docs.microsoft.com/en-us/rest/api/compute/virtualmachines/get" \t "_blank)

1. <https://cseweb.ucsd.edu/~savage/papers/CCS09.pdf>. Accessed July 2, 2020.
2. Wait a minute! A fast, Cross-VM attack on AES Gorka Irazoqui, Mehmet Sinan Inci, Thomas Eisenbarth, and Berk Sunar Worcester Polytechnic Institute, Worcester, MA, USA – Accessed August 6,2020