Exploiting New Vulnerabilities in Managed Cloud Services (version 1.0)

**Cloud Service Label:  PaaS, SaaS**

Description

Cloud Service Providers (CSPs) have various services within their cloud environments that can be seamlessly integrated and utilized for a customer’s needs. The purpose of managed cloud services is to remove the need to install and manage common software applications. These managed services move the responsibility of maintaining, patching, and updating to the CSPs and the vendors that provide the managed service.

Managed cloud services can be used at both the infrastructure and application levels. The infrastructure level includes services for providing architecture recommendations, system administration, monitoring, DNS management, Kubernetes support and many others. The application level provides support for packages like Ansible, Elasticsearch, LogStash, database management with MongoDB, and various other services as well.

While managed cloud services are generally thought to be more secure than running a custom or IaaS hosted application or tool, they are still susceptible to vulnerabilities and exploitation and often provide less visibility to customers than comparable IaaS-hosted versions. The Cloud Service Provider will normally remove the worry of vulnerability management through automatic patching and updating, but it is still important to be aware of potential vulnerabilities through managed cloud services, because these could still lead to exploitation of customer assets.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Azure Sphere Talos Vulnerabilities | A blog article put out by Talos Intelligence highlights several vulnerabilities found in the Azure Sphere service, which is a cloud System on a Chip (SoC) platform designed to implement IoT application security. These vulnerabilities include information disclosure, unsigned code execution, socket memory corruption, denial of service, and privilege escalation. |

Mitigations

|  |  |  |
| --- | --- | --- |
| **Mitigations** | | **Description** |
| Audit |  | Perform periodic audits to ensure that best security practices are implemented and that unusual /unexplainable events are not occurring |
|  | *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**](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**](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**](https://cloud.google.com/logging/docs/audit)**.** |
| Setting IAM Policies and Permissions |  | Implement least privilege and assign roles and permissions to users as necessary. |
|  | *AWS* | Amazon’s article for IAM security best practices in AWS covers topics including creating individual IAM users, using AWS managed policies, roles, frequent key rotation and others. Full details can be found at [**https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html**](https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html)**.** |
|  | *Azure* | Microsoft’s article for IAM security best practices in Azure covers topics including centralizing identity management, turning on conditional access, use role-based access control, using Azure AD for storage authentication, and others. Full details can be found at [**https://docs.microsoft.com/en-us/azure/security/fundamentals/identity-management-best-practices**](https://docs.microsoft.com/en-us/azure/security/fundamentals/identity-management-best-practices)**.** |

Detection

|  |  |
| --- | --- |
| **Detection** | **Description** |
| Leverage IDS Rules to independently detect unusual network events within the cloud | Implementing Snort rules 54501 – 53504 will detect attempts at exploitations specific to the above Azure Sphere vulnerabilities. |
| 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* |
| 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* |
| Monitoring for Regional Activity | Tools like Splunk or even CloudSploit have the ability to alert based on region and ingest CloudTrail logs. In CloudSploit, a plugin called EC2 Max Count can be configured to alert after a certain threshold of EC2 instances is met. Real-Time Events service is another feature of CloudSploit that allows alerts for activity in unused regions. |

References

1. <https://blog.talosintelligence.com/2020/07/vuln-spotlight-azure-sphere-july-2020.html> Accessed August 11, 2020.