Cloud Security Assessment-Knee Balancer

**Index**

# Infrastructure Security

**Subscriptions:**

1. Subscription Name: Stryker-Dev/Test

Subscription id:

Status: Active

1. Microsoft Defender for cloud

Subscription: No

**Resource Group: Knee-Balancer**

Security center

Recommendation -1

|  |  |  |
| --- | --- | --- |
| **Web apps should request an SSL certificate for all incoming requests** | | |
| **Severity** | Medium | |
| **Tactics and techniques** | Initial access (Trusted Relationship) | |
| **Affected Resources** | Unhealthy resource | Name: kneebalancer-dev |
| Subscription: Stryker-Dev/Test |
| **Resource type** | Web application | |
| **Description** | | |
| Client certificates allow for the app to request a certificate for incoming requests. Only clients that have a valid certificate will be able to reach the app. | | |
| **Remediation** | | |
| Manual remediation:  To set Client Certificates for your Web App: 1. Navigate to Azure App Service 2. Select Configuration 3. Go to the General Settings tab 4. Set Incoming Client Certificates to Require. For more information, visit here: <https://aka.ms/auth-tls> | | |

Recommendation -2

|  |  |  |
| --- | --- | --- |
| **Authentication should be enabled on your web app** | | |
| **Severity** | Low | |
| **Affected Resources** | Unhealthy resource | Name: kneebalancer-dev |
| Subscription: Stryker-Dev/Test |
| **Resource type** | Web application | |
| **Description** | | |
| Azure App Service Authentication is a feature that can prevent anonymous HTTP requests from reaching the web app, or authenticate those that have tokens before they reach the web app | | |
| **Remediation** | | |
|  | | |

Recommendation -3

|  |  |  |
| --- | --- | --- |
| **Ensure that ‘HTTP Version’ is the latest, if used to run the Web app** | | |
| **Severity** | Low | |
| **Affected Resources** | Unhealthy resource | Name: kneebalancer-dev |
| Subscription: Stryker-Dev/Test |
| **Resource type** | Web application | |
| **Description** | | |
| Periodically, newer versions are released for HTTP either due to security flaws or to include additional functionality. Using the latest HTTP version for web apps to take advantage of security fixes, if any, and/or new functionalities of the newer version. Currently, this policy only applies to Linux web apps. | | |
| **Remediation** | | |
|  | | |

Recommendation -4

|  |  |  |
| --- | --- | --- |
| **Managed identity should be used in web apps** | | |
| **Severity** | Medium | |
| **Tactics and techniques** | Credential access (Unsecured Credentials) | |
| **Affected Resources** | Unhealthy resource | Name: kneebalancer-dev |
| Subscription: Stryker-Dev/Test |
| **Resource type** | Web application | |
| **Description** | | |
| For enhanced authentication security, use a managed identity. On Azure, managed identities eliminate the need for developers to have to manage credentials by providing an identity for the Azure resource in Azure AD and using it to obtain Azure Active Directory (Azure AD) tokens. | | |
| **Remediation** | | |
| Manual remediation:  To create a managed identity for your web app: 1. Go to the App Service for your API app 2. Scroll to the Settings group in the left navigation 3. Select Identity 4. Use System assigned or User assigned identity following the steps described in this doc: <https://aka.ms/managed-identity> | | |

Recommendation -5

|  |  |  |
| --- | --- | --- |
| **Diagnostic logs in App Service should be enabled** | | |
| **Severity** | Medium | |
| **Affected Resources** | Unhealthy resource | Name: kneebalancer-dev |
| Subscription: Stryker-Dev/Test |
| **Resource type** | Web application | |
| **Description** | | |
| Audit enabling of diagnostic logs on the app. This enables you to recreate activity trails for investigation purposes if a security incident occurs or your network is compromised. | | |
| **Remediation** | | |
| Manual remediation:  To enable resource logs for an App Service: 1. Navigate to your App Service. 2. Go to 'Diagnostic Settings' tab. 3. Enable necessary auditing services for your specified apps. For more information, please go to <https://aka.ms/enabling-diagnostic-settings>. | | |

Recommendation -6

|  |  |  |
| --- | --- | --- |
| **Web Application should only be accessible over HTTPS** | | |
| **Severity** | Medium | |
| **Tactics and techniques** | Credential access (Network Sniffing)  Discovery (Network Sniffing) | |
| **Affected Resources** | Unhealthy resource | Name: kneebalancer-dev |
| Subscription: Stryker-Dev/Test |
| **Resource type** | Web application | |
| **Description** | | |
| Use of HTTPS ensures server/service authentication and protects data in transit from network layer eavesdropping attacks. | | |
| **Remediation** | | |
| Quick fix: Select the unhealthy resources and click “Fix” to launch “Quick fix” remediation. [Learn more >](https://docs.microsoft.com/azure/security-center/security-center-remediate-recommendations?WT.mc_id=Portal-Microsoft_Azure_Security#quick-fix-remediation) Note: After the process completes, it may take up to 30 min until your resources move to the ‘healthy resources’ tab. | | |

Recommendation -7

|  |  |  |
| --- | --- | --- |
| **FTPS should be required in web apps** | | |
| **Severity** | High | |
| **Tactics and techniques** | Credential access (Network Sniffing)  Discovery (Network Sniffing) | |
| **Affected Resources** | Unhealthy resource | Name: kneebalancer-dev |
| Subscription: Stryker-Dev/Test |
| **Resource type** | Web application | |
| **Description** | | |
| Enable FTPS enforcement for enhanced security | | |
| **Remediation** | | |
| Manual remediation:  To ensure enforcement of FTPS only for your web app: 1. Go to the App Service for your API app 2. Select Configuration, and go to the General Settings tab 3. In FTP state, select FTPS only. For more information, visit here: <https://aka.ms/deploy-ftp> | | |

Reference link to export secure score:

[Security recommendations in Microsoft Defender for Cloud | Microsoft Docs](https://docs.microsoft.com/en-us/azure/defender-for-cloud/review-security-recommendations)

[Secure Score Over Time - Microsoft Azure](https://portal.azure.com/#blade/AppInsightsExtension/WorkbookViewerBlade/ComponentId/Azure%20Security%20Center/GalleryResourceType/Azure%20Security%20Center/ConfigurationId/community-Workbooks%2FAzure%20Security%20Center%2FSecure%20Score)

To use this Secure Score Over Time workbook, you'll need to configure **continuous export** to export data to a Log Analytics workspace:

1. From Defender for Cloud sidebar, select **Environment settings**.
2. Select the specific subscription for which you want to configure the data export.
3. From the sidebar of the settings page for that subscription, select **Continuous export**.
4. Set the export targed to **Log Analytics workspace**.
5. Select the following data types: **Security recommendations** and **Secure score**.
6. From the export frequency options, select **Streaming updates** and **Snapshots (Preview)**.
7. Select **Save**.

**Notes**

* To get full visibility, wait at least one week for the first snapshot to be exported.
* To configure continuous export across your organization, use the supplied Azure Policy 'DeployIfNotExist' policies described [here](https://docs.microsoft.com/azure/defender-for-cloud/continuous-export?tabs=azure-policy&WT.mc_id=Portal-fx#set-up-a-continuous-export).

**Microsoft defender for cloud:**

Overview:

**Graphical user interface, text

Description automatically generated**

Click on the Azure subscriptions

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Next go to Assessed resources

Graphical user interface, text, application, email

Description automatically generated

-Select the resource “kneebalancer-dev”

Graphical user interface, application, table

Description automatically generated

Go to Active recommendations

Graphical user interface, text, application, email

Description automatically generated

**Task**

Azure Infrastructure

1. Identifying the resource group
2. List down the resources present in the resource grp
3. Identify & list down the unsecure resources
4. List down the recommendations of unsecure resource

Storage