# Threat Modeling Report

Created on 11/15/2020 7:38:38 PM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

Assumptions:

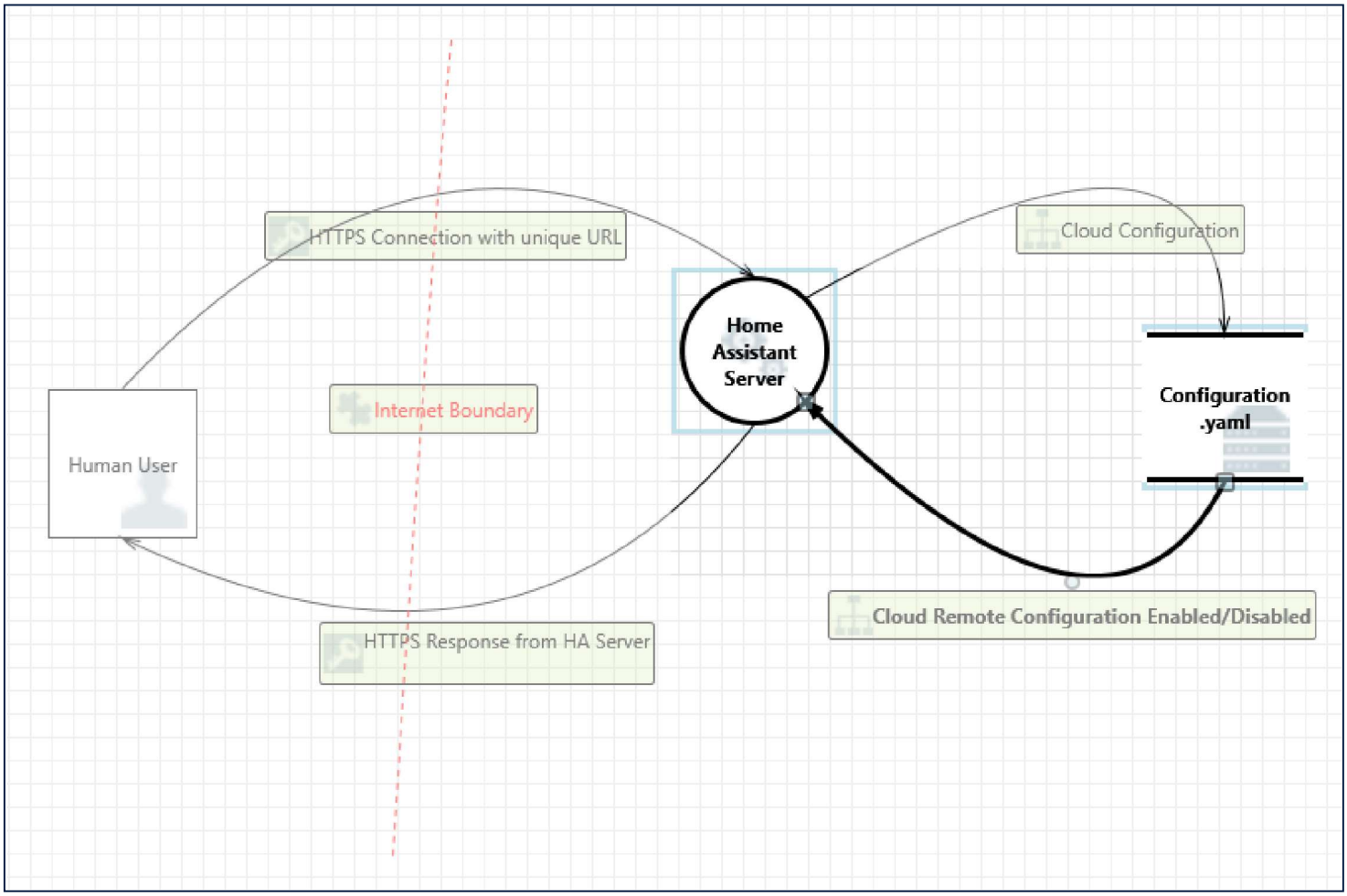
External Dependencies:

## Threat Model Summary:

| | |
|---|---|
| Not Started | 0 |
| Not Applicable | 3 |
| Needs Investigation | 1 |
| Mitigation Implemented | 11 |
| Total | 15 |
| Total Migrated | 0 |

---

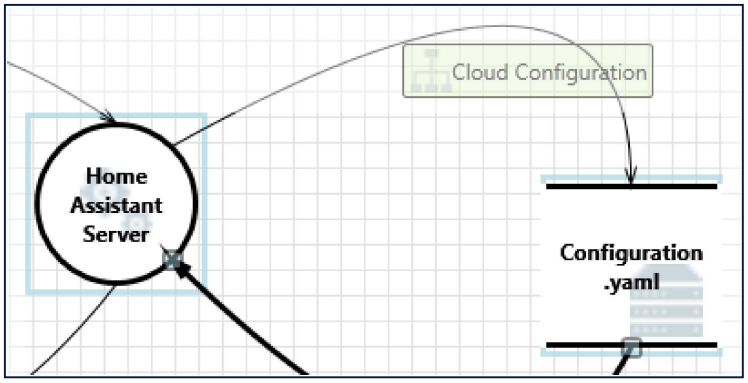
## Diagram: Diagram 1




## Diagram 1 Diagram Summary:

| | |
|---|---|
| Not Started | 0 |
| Not Applicable | 3 |
| Needs Investigation | 1 |
| Mitigation Implemented | 11 |
| Total | 15 |
| Total Migrated | 0 |

## Interaction: Cloud Configuration




1. Spoofing of Destination Data Store Configuration.yaml [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Configuration.yaml may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Configuration.yaml. Consider using a standard authentication mechanism to identify the destination data store.

Justification: This is an internal configuration file. Any improper data disclosures is a result of the Home Assistant Server already being compromised.

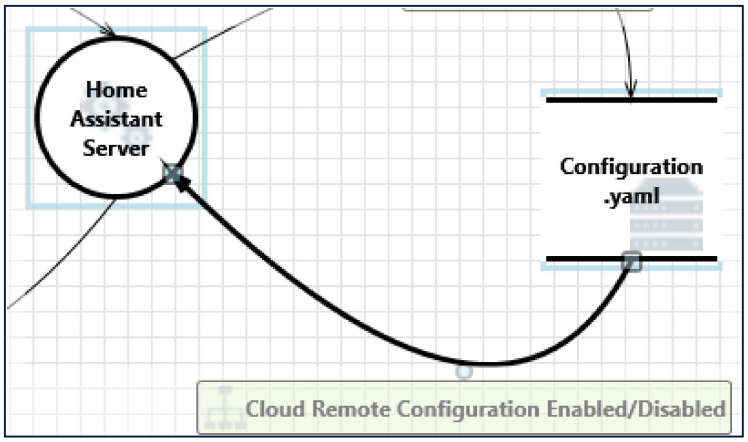
2. Potential Excessive Resource Consumption for Home Assistant Server or Configuration.yaml [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: Does Home Assistant Server or Configuration.yaml take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.

Justification: This is an internal configuration file. Any improper data disclosures is a result of the Home Assistant Server already being compromised.

## Interaction: Cloud Remote Configuration Enabled/Disabled




3. Spoofing of Source Data Store Configuration.yaml [State: Mitigation Implemented] [Priority: Medium]

Category: Spoofing

Description: Configuration.yaml may be spoofed by an attacker and this may lead to incorrect data delivered to Home Assistant Server. Consider using a standard authentication mechanism to identify the source data store.

Justification: This is an internal configuration file. Any improper data disclosures is a result of the Home Assistant Server already being compromised.

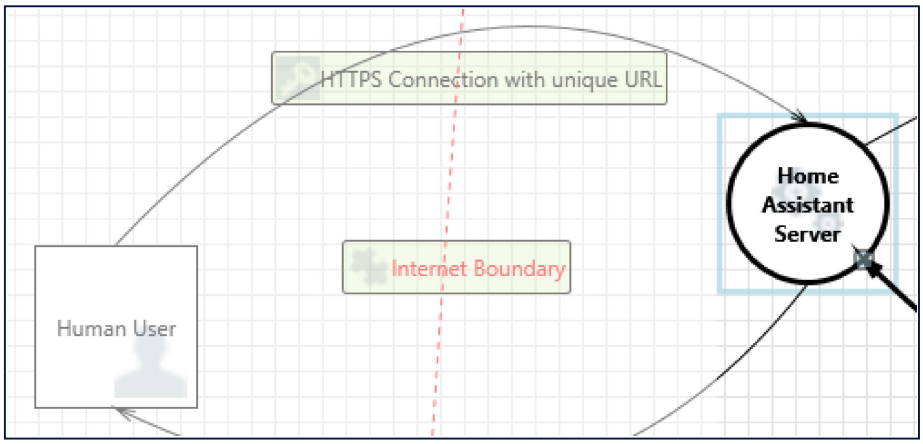
4. Weak Access Control for a Resource [State: Mitigation Implemented] [Priority: Medium]

Category: Information Disclosure

Description: Improper data protection of Configuration.yaml can allow an attacker to read information not intended for disclosure. Review authorization settings.

Justification: This is an internal configuration file. Any improper data disclosures is a result of the Home Assistant Server already being compromised.

## Interaction: HTTPS Connection with unique URL




### 5. Spoofing the Human User External Entity [State: Mitigation Implemented] [Priority: High]

**Category:** Spoofing

**Description:** Human User may be spoofed by an attacker and this may lead to unauthorized access to Home Assistant Server. Consider using a standard authentication mechanism to identify the external entity.

**Justification:** Outside of Scope as the routing is handled by a third party.

### 6. Elevation Using Impersonation [State: Not Applicable] [Priority: Medium]

**Category:** Elevation Of Privilege

**Description:** Home Assistant Server may be able to impersonate the context of Human User in order to gain additional privilege.

**Justification:** Home Assistant Users are verified from the auth_provider process

### 7. Potential Data Repudiation by Home Assistant Server [State: Mitigation Implemented] [Priority: High]

**Category:** Repudiation

**Description:** Home Assistant Server claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

**Justification:** Home Assistant Server keeps logs of authenticated users.

### 8. Potential Process Crash or Stop for Home Assistant Server [State: Needs Investigation] [Priority: High]

**Category:** Denial Of Service

**Description:** Home Assistant Server crashes, halts, stops or runs slowly; in all cases violating an availability metric.

**Justification:** Approporate routing is handeled by third party Nobu-Casa, but if their services hit the local Home Assistant Server repeatily does this cause Availability to degrade?

### 9. Data Flow HTTPS Connection with unique URL Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: Mitigated by Nobu-Casa Third Party Proxy Services.

### 10. Home Assistant Server May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Human User may be able to remotely execute code for Home Assistant Server.

Justification: Mitigated by Nobu-Casa Third Party Proxy Services.

### 11. Elevation by Changing the Execution Flow in Home Assistant Server [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into Home Assistant Server in order to change the flow of program execution within Home Assistant Server to the attacker's choosing.

Justification: Mitigated by Nobu-Casa Third Party Proxy Services.

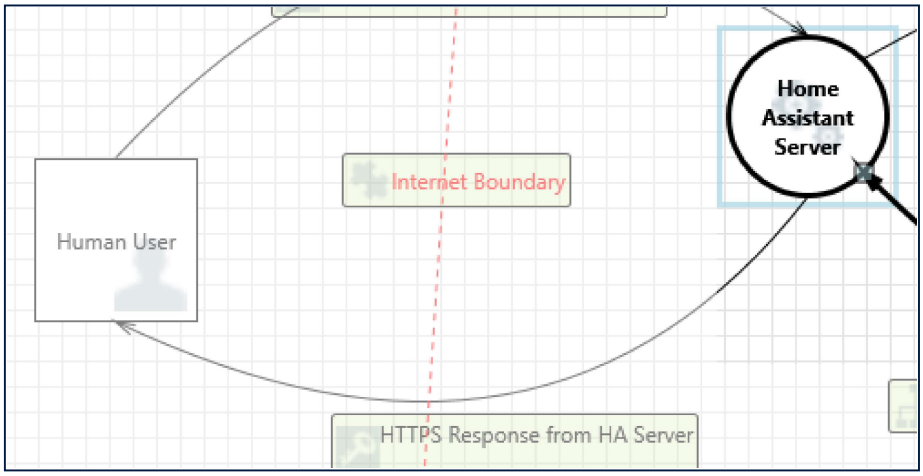
### 12. Cross Site Request Forgery [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Cross-site request forgery (CSRF or XSRF) is a type of attack in which an attacker forces a user's browser to make a forged request to a vulnerable site by exploiting an existing trust relationship between the browser and the vulnerable web site. In a simple scenario, a user is logged in to web site A using a cookie as a credential. The other browses to web site B. Web site B returns a page with a hidden form that posts to web site A. Since the browser will carry the user's cookie to web site A, web site B now can take any action on web site A, for example, adding an admin to an account. The attack can be used to exploit any requests that the browser automatically authenticates, e.g. by session cookie, integrated authentication, IP whitelisting. The attack can be carried out in many ways such as by luring the victim to a site under control of the attacker, getting the user to click a link in a phishing email, or hacking a reputable web site that the victim will visit. The issue can only be resolved on the server side by requiring that all authenticated state-changing requests include an additional piece of secret payload (canary or CSRF token) which is known only to the legitimate web site and the browser and which is protected in transit through SSL/TLS. See the Forgery Protection property on the flow stencil for a list of mitigations.

Justification: Mitigated by Nobu-Casa Third Party Proxy Services.

## Interaction: HTTPS Response from HA Server




13. Spoofing of the Human User External Destination Entity [State: Not Applicable] [Priority: High]

Category: Spoofing

Description: Human User may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Human User. Consider using a standard authentication mechanism to identify the external entity.

Justification: Outside of Scope as the routing is handled by a third party.

14. External Entity Human User Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Human User claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: Home Assistant Server keeps logs of authenticated users.

15. Data Flow HTTPS Response from HA Server Is Potentially Interrupted [State: Not Applicable] [Priority: Low]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: Outside of Scope as the routing is handled by a third party.