

home-assistant / core Public

<> Code Issues 2.9k Pull requests 676 Actions Projects Security and o

Stored XSS in Map-card through malicious device name

Moderate bramkragten published GHSA-r584-6283-p7xc last week

Package

 Home Assistant (pip)

Affected versions

2020.02 to 2026.01

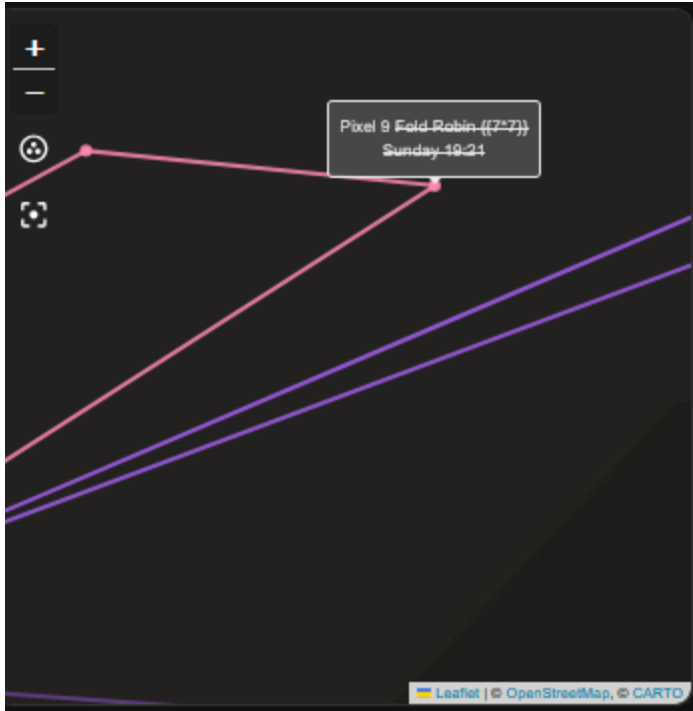
Patched versions

2026.01

Description

Summary

An authenticated party can add a malicious name to their device entity, allowing for Cross-Site Scripting attacks against anyone who can see a dashboard with a Map-card which includes that entity. It requires that the victim hovers over an information point (The lines or the dots representing that device's movement, as shown in the screenshot below, with the example showing a html-injection using `<s>` to strikethrough the text)



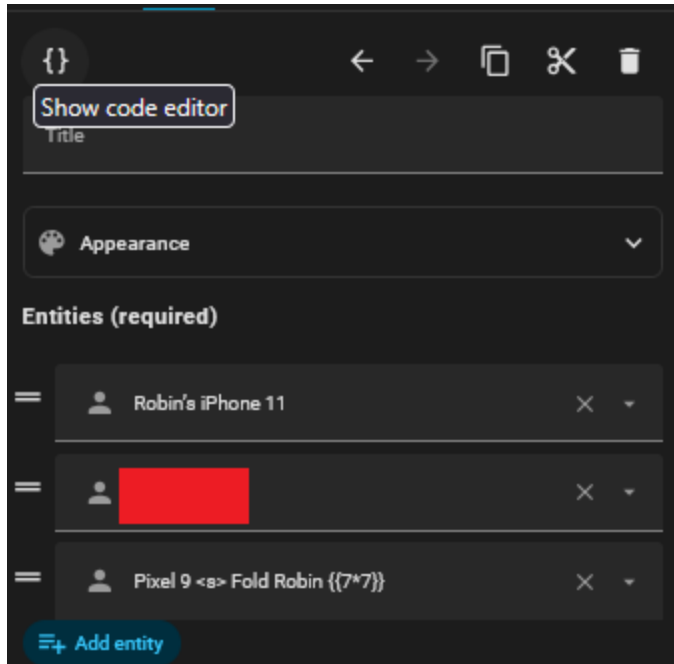
This allows an authenticated user to execute JavaScript in the context of any other users accessing a dashboard.

Details

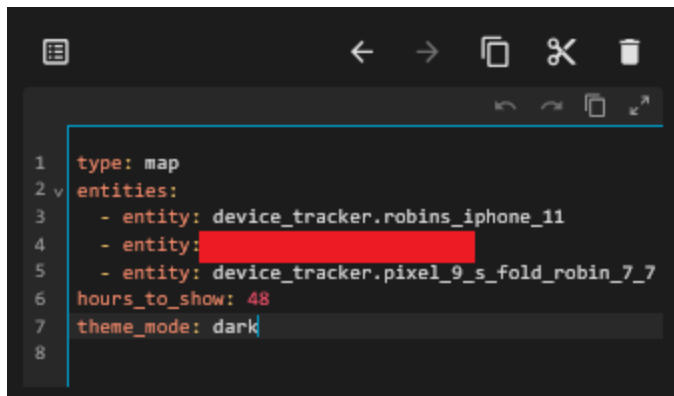
The vulnerability exists in the map-card by adding a malicious entity and having the property `hours_to_show` set.

See example below, with the malicious entity being `Pixel 9 <s> Fold Robin {{7*7}}`:

Map card with malicious device entity:



YAML-view of same card:

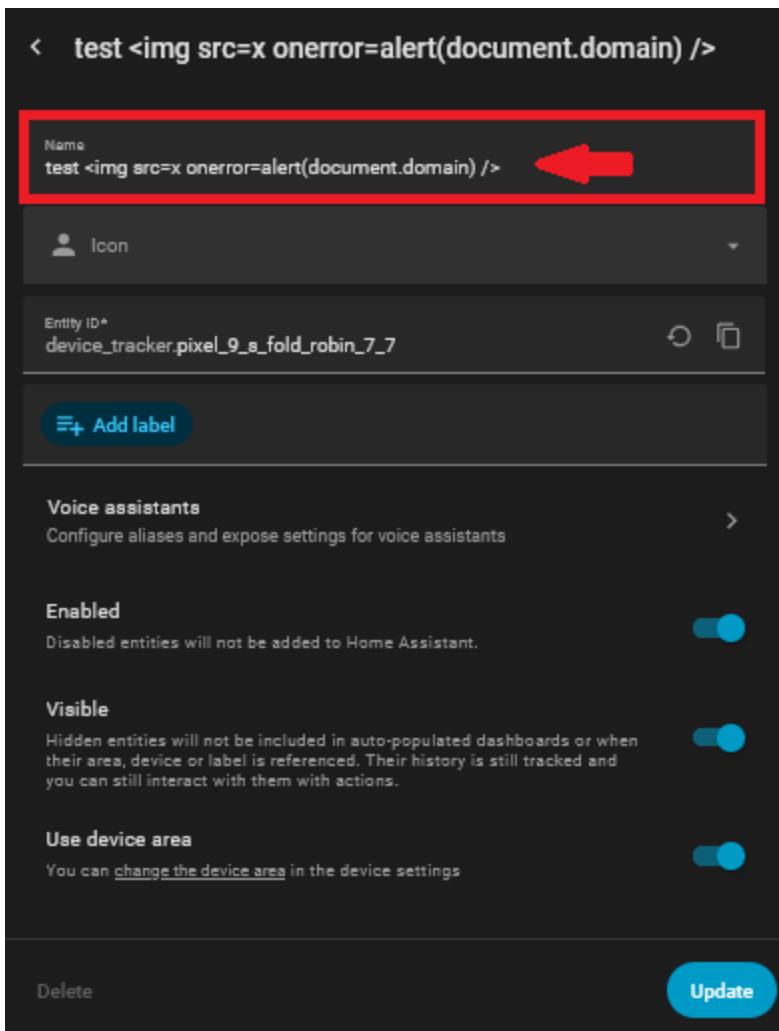
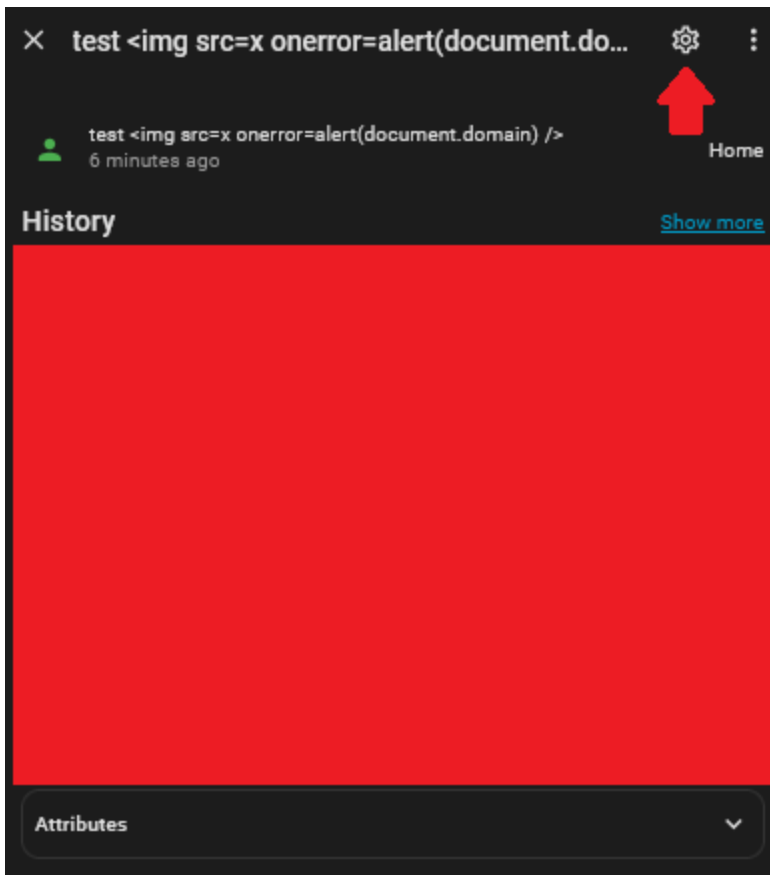


This issue largely resembles the issue documented in: [CVE-2025-62172](https://github.com/home-assistant/core/security/advisories/GHSA-2025-62172), but with an entity which can be displayed in a Map, instead of in an energy-dashboard.

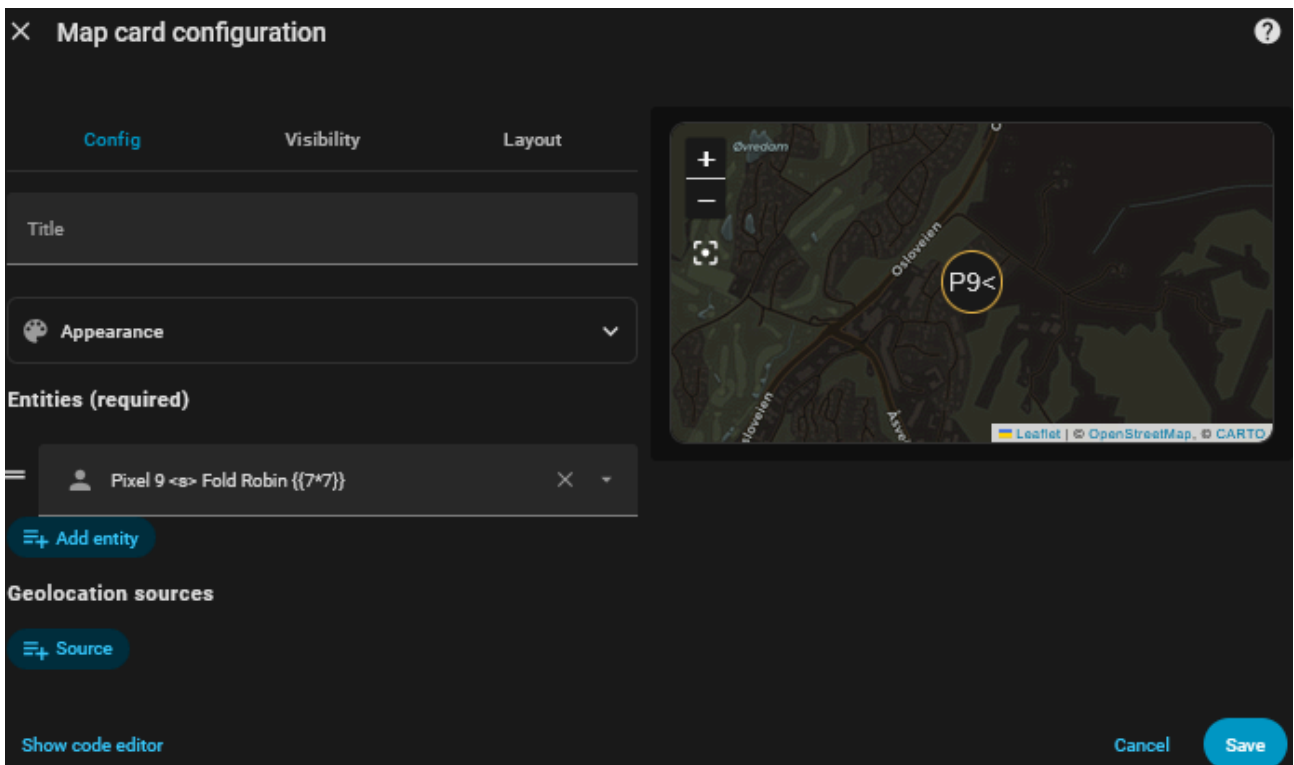
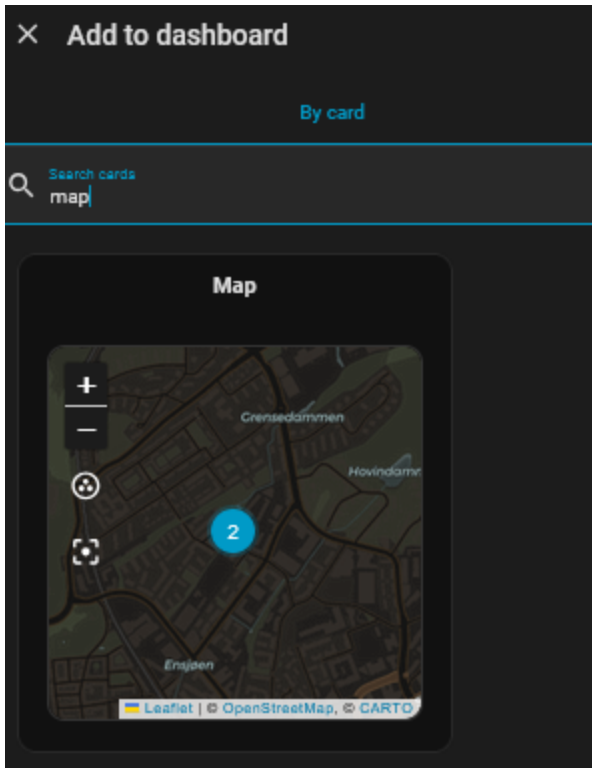
PoC

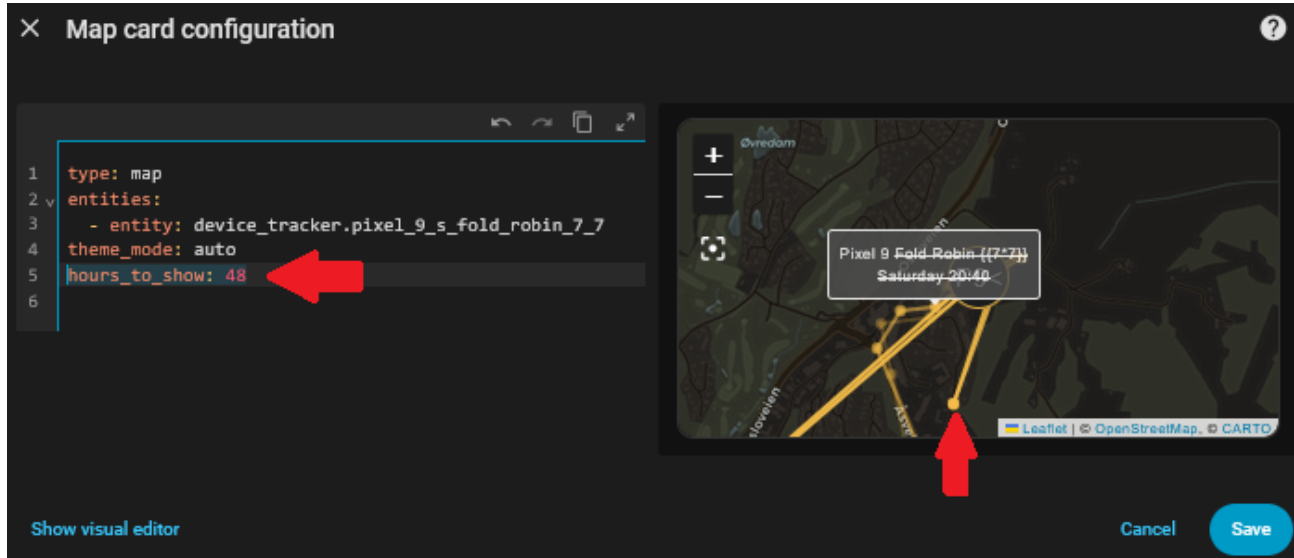
1. Register a new sensor (or device) or change the name of an existing one, which provides a location
2. Change the name to something malicious, for example `test `

For a new entity, it should work when setting the name. For old entities, go here:



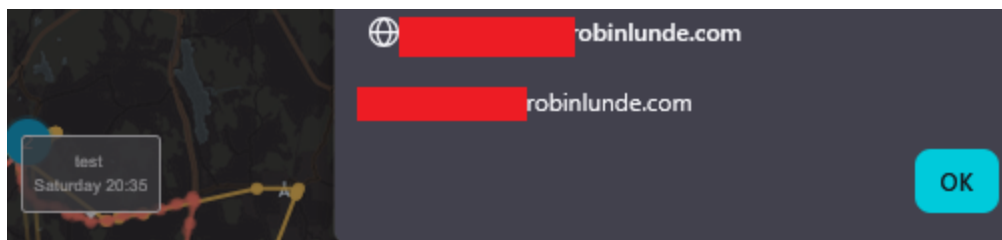
3. Add the entity to a map card, which has the "hours to show"-attribute set, to display movement history





(The left arrow showing the custom setting, and the right arrow showing a data point which needs to be hovered)

- The payload executes when hovering a data-point (here shown with an "alert(document.domain)"-payload)



Impact

The impact of this vulnerability is that a user can target other users of the system and perform account takeover through client side exploitation of XSS.

In the context of this system, I believe the vulnerability to be less impactful than the CVSS metric describes, as it requires a specific setup (map-card with attribute `hours_to_show` set, as this brings up the trail). It is interesting to note that any user who sets this attribute, will be highly likely to trigger the vulnerability through normal use. It also has no potential for being imported through seemingly innocent integrations and can only be set explicitly by another invited user, a device name, a cloud service or through social engineering. Other devices which has the same sensor can trigger the same vulnerability, and I expect there to exist cloud-based devices that would enable a threat actor to deliver the payload remotely.

Suggested CVSS score:

CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:A/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:P

Suggested criticality: **Medium**

Credit: Robin Lunde - <https://robinlunde.com>

Severity

Moderate


CVE ID

CVE-2026-33044

Weaknesses

▶ CWE-80

Credits

 pwnpanda

Reporter