Stored XSS in history-graphs

Moderate **bramkragten** published **GHSA-46j8-vpx8-6p72** last week

Package

Home Assistant (pip)

Affected versions

2025.02 to 2026.01

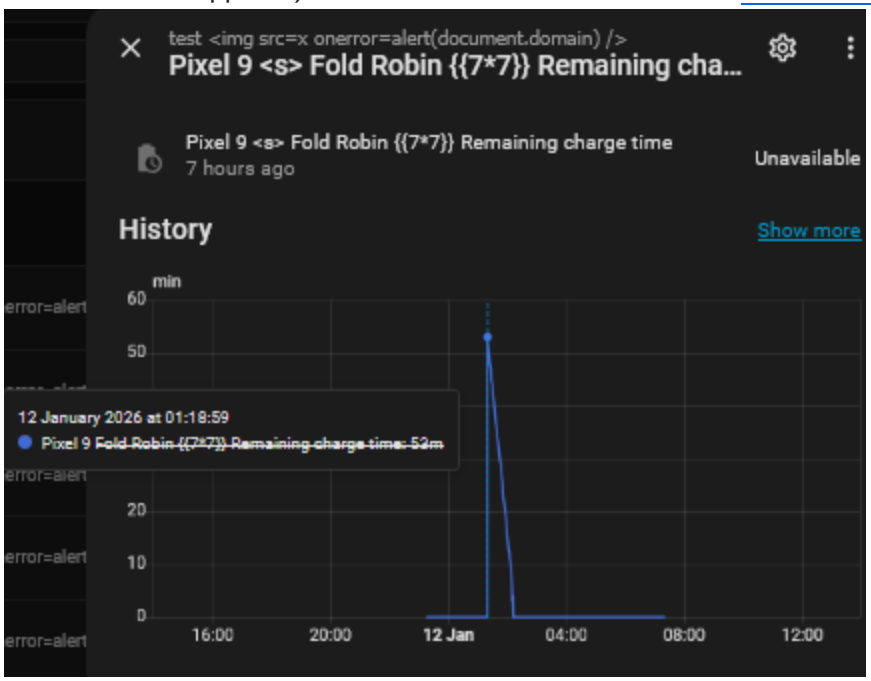
Patched versions

2026.01

Description

Summary

I have found that the "remaining charge time"-sensor for mobile phones (imported/included from Android Auto it appears) is vulnerable to the same issue as CVE-2025-62172.



I believe that also indicates that any sensor showing their name in the history-graph, is likely to be vulnerable to this issue.

Details

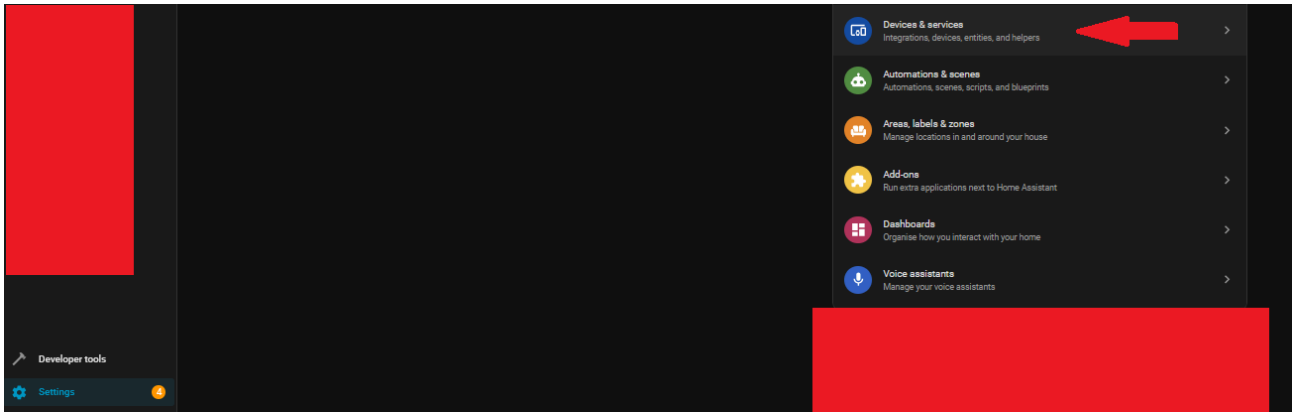
I have found another entity which displays the same behavior as in this issue: CVE-2025-62172

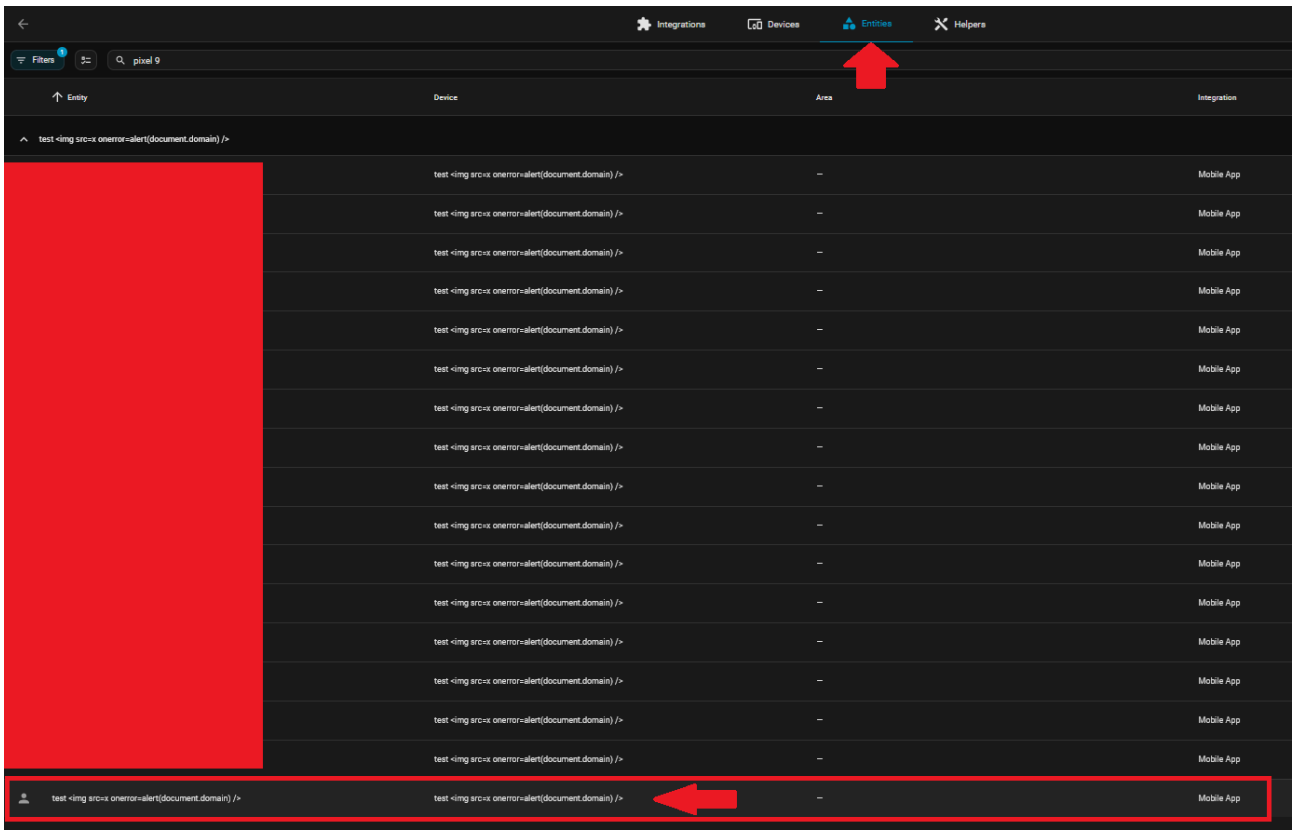
The History-graph card will sometimes display the name of the entity it is displaying, when the graph is shown as a line with values on the x and y axis. This appears to be vulnerable to Cross-Site scripting (*XSS*) as it does not have any output escaping or sanitization.

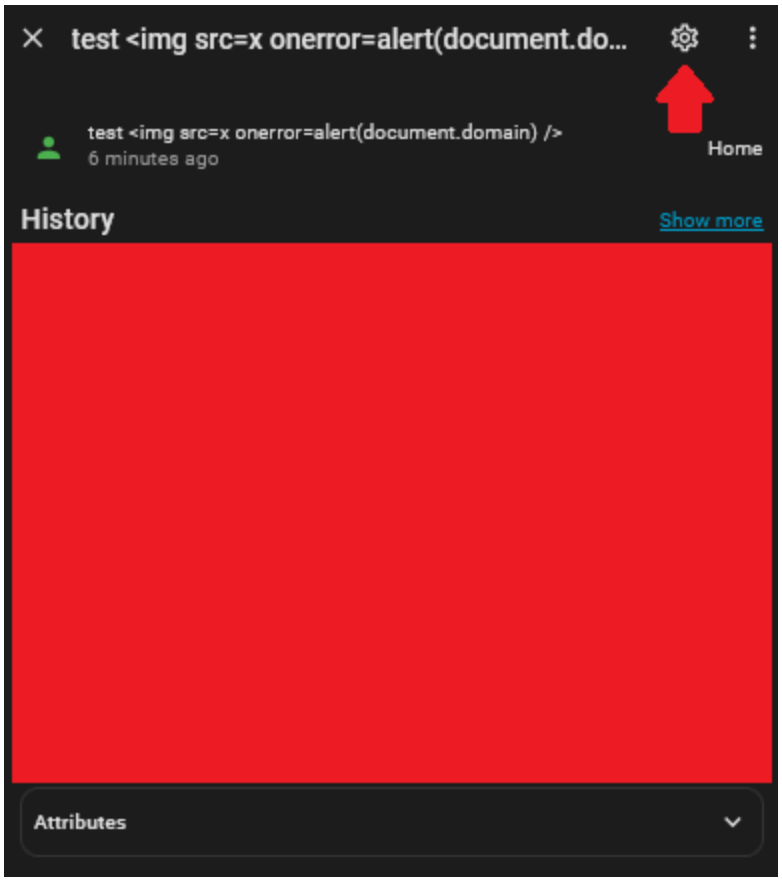
The PoC in this instance only shows HTML-injection in the form of the `<s>` -tag being rendered as strike through, but the vulnerability also allows for injecting arbitrary tags which execute JavaScript, like the example given in the PoC description below.

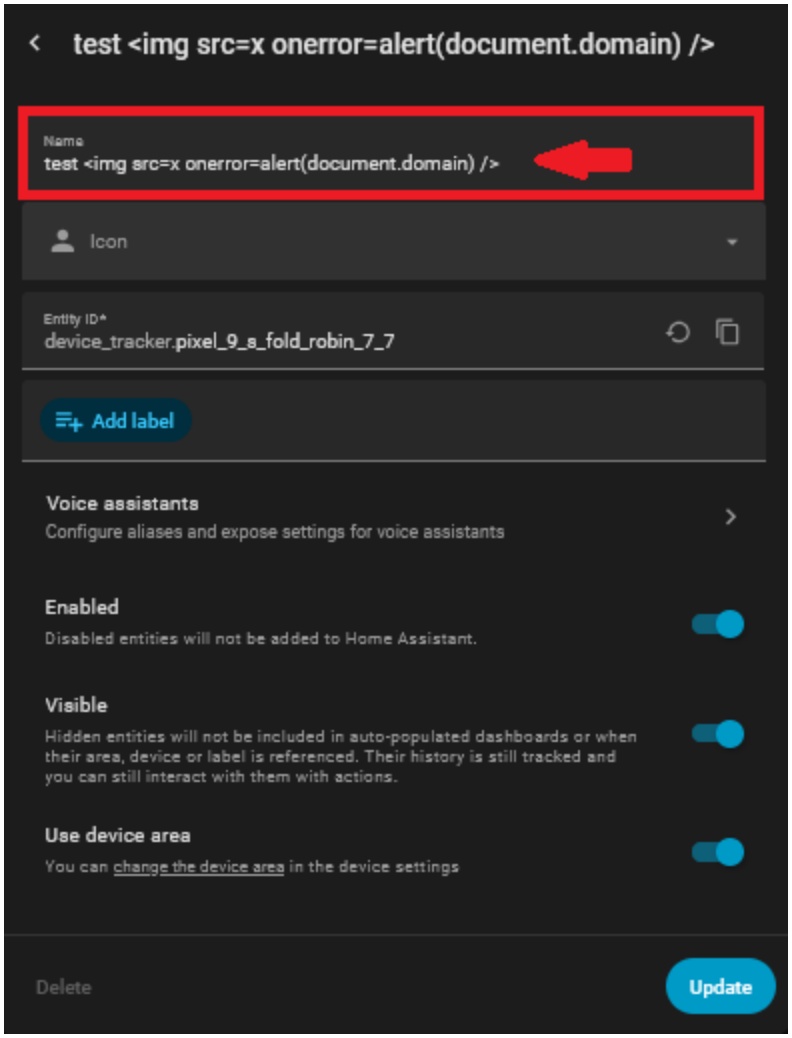
PoC

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 <img src=x onerror=alert(document.domain) />`
   For a new entity, it should work when setting the name. For old entities, go here:



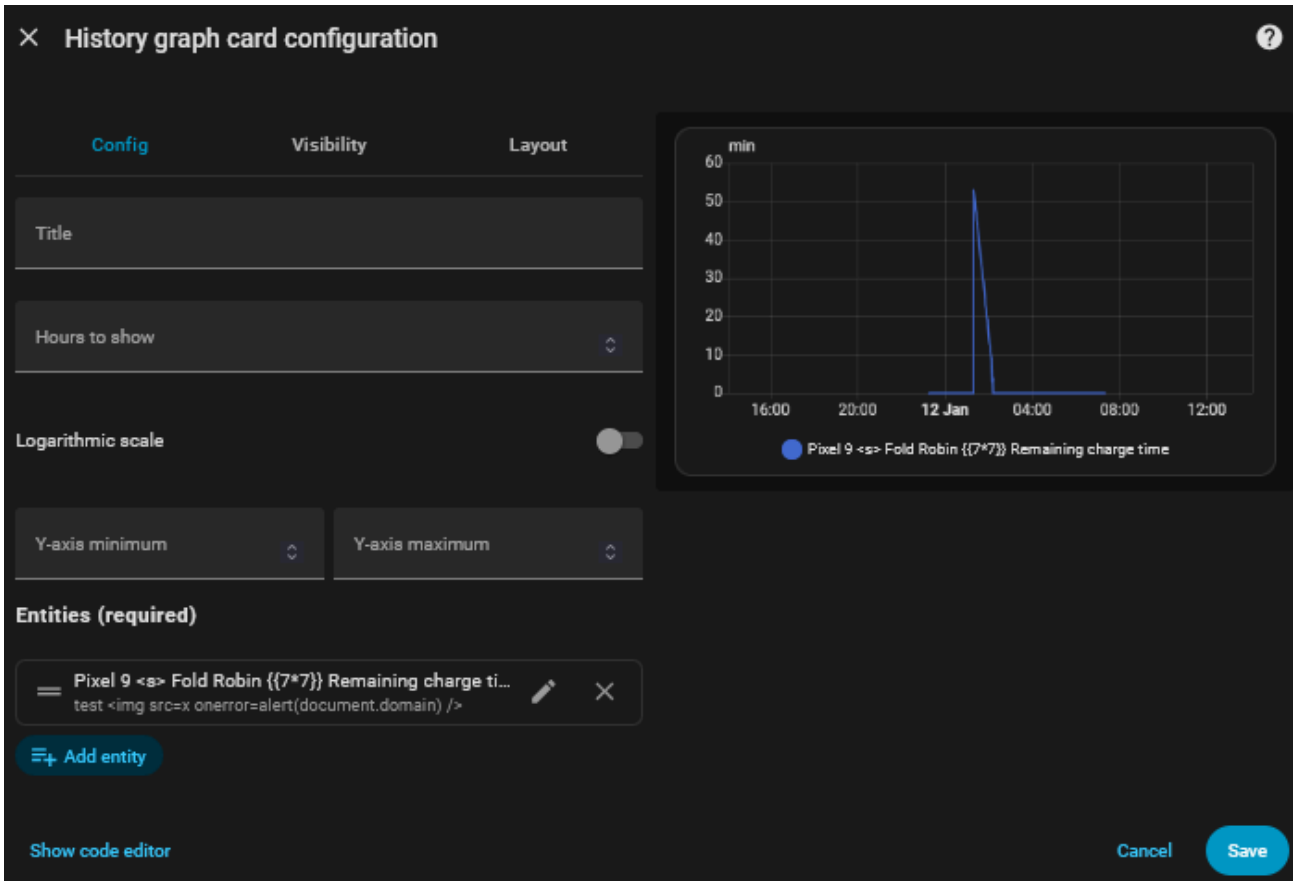



test <img src=x onerror=alert(document.do...
test
6 minutes ago
Home
History
Show more
Attributes

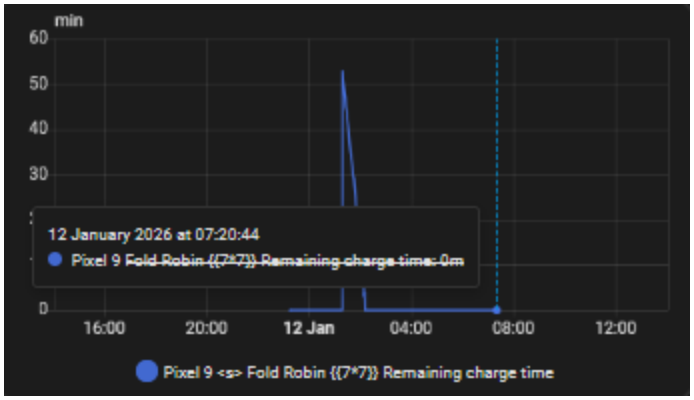

test
Name
test
Icon
Entity ID*
device_tracker.pixel_9_s_fold_robin_7_7
Add label
Voice assistants
Configure aliases and expose settings for voice assistants
Enabled
Disabled entities will not be added to Home Assistant.
Visible
Hidden entities will not be included in auto-populated dashboards or when their area, device or label is referenced. Their history is still tracked and you can still interact with them with actions.
Use device area
You can change the device area in the device settings
Delete
Update

PS: the example pictures show changing the name of the device-tracker entity, which is wrong. Just change the name of the `remaining charge time`-sensor in order to validate this finding

3. Add a history graph card with the malicious sensor



5. Hover the graph for payload execution



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. It is not displayed anywhere by default, it is not natural to display this history graph, and it also has no potential for being imported through seemingly innocent integrations. It also appears to rely on having used/using Android Auto. Other devices which has the same sensor can trigger the same vulnerability, and I expect there to exists 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-2026-33045

Weaknesses

▶ CWE-80

Credits

pwnpanda Reporter