

 PebbleTemplates / pebble Public[Code](#) [Issues 25](#) [Pull requests 2](#) [Discussions](#) [Actions](#) [Security and compliance](#)[New issue](#)

# GHSA-p75g-cxfj-7wrx: Unpatched Arbitrary Local File Inclusion (LFI) Vulnerability via `include` macro when `PebbleTemplate` created with `PebbleEngine#getLiteralTemplate` #688

Closed#715Milestone 4.1.0

JLLeitschuh opened on Feb 24, 2025






This issue is to track the now disclosed and, as of this post, unfixed vulnerability in Pebble Templates.



[GHSA-p75g-cxfj-7wrx](#)


## Report Timeline

Vulnerability was reported under the Open Source Security Foundation (OpenSSF) [Model Outbound Vulnerability Disclosure Policy: Version 0.1](#).



- [Jul 15, 2024](#) Maintainer Contacted to enable private vulnerability reporting
- [Jul 18, 2024](#) I opened a GHSA to report this vulnerability to the maintainer <https://github.com/PebbleTemplates/pebble/security/advisories/GHSA-7c6h-hmf9-7wj7> (private link)
- Jul 29, 2024 GHSA updated to ping maintainer about vulnerability, no response
- Oct 1, 2024 GHSA updated to ping maintainer about vulnerability, no response
- Nov 15, 2024 GHSA updated to inform maintainer that disclosure timeline had lapsed, no response.
- Feb 19, 2025 GHSA updated to inform maintainer that disclosure would occur imminently, no response.
- Feb 24, 2025 a new GHSA was created to disclose this vulnerability **without a patch available** ([GHSA-p75g-cxfj-7wrx](#)).


  **kbsteere** mentioned this [on Mar 4, 2025](#)  
 [dependency-track/advisory update wolfi-dev/advisories#13627](#)

  **ebussieres** closed this as [completed](#) [on Nov 22, 2025](#)



 JLLeitschuh on Nov 22, 2025 Author ...


Was this fixed?

  **ebussieres** closed this as [not planned](#) [on Nov 23, 2025](#)

 ebussieres on Nov 23, 2025 Member ...



I think that if we remove the `getLiteralTemplate` which uses a `StringLoader`, it would be sufficient to fix this vulnerability. Originally it was to address this [issue](#) but I'm comfortable to remove it. Don't think it's heavily used.

  **ebussieres** reopened this [on Nov 23, 2025](#)

 ebussieres on Nov 23, 2025 · edited by ebussieres Edits ... Member ...


[@JLLeitschuh](#) What do you think ?



Ref: [#715](#)

  **ebussieres** added this to the [4.0.1 milestone](#) [on Nov 23, 2025](#)

  **ebussieres** mentioned this [on Nov 23, 2025](#)

 [CVE-2025-1686 vulnerability #689](#)

 [CVE-2025-1686 #715](#)

  **ebussieres** closed this as [completed](#) in [#715](#) [on Dec 11, 2025](#)

[Sign up for free](#) to join this conversation on **GitHub**. Already have an account? [Sign in to comment](#)

## Metadata

### Assignees

No one assigned

### Labels

No labels

### Type

No type

### Projects

No projects

### Milestone



✔ **4.1.0**

Closed on Dec 11, 2025, 100% complete

### Relationships

None yet

### Development

 [CVE-2025-1686](#)  
PebbleTemplates/pebble  
 **4.1.0**

### Participants



