New issue

# Report a Security Vulnerability #680

Closed

JLLeitschuh opened on Jul 15, 2024

Hello,

My name is Jonathan Leitschuh, I'm a Principal Software Security Researcher at Chainguard. I'd like to report a potential security vulnerability in the Pebble template engine.

Would you be so kind as to enable GitHub Private Vulnerability Reporting? I'd like to privately disclose the details to you there.
https://docs.github.com/en/code-security/security-advisories/guidance-on-reporting-and-writing-information-about-vulnerabilities/privately-reporting-a-security-vulnerability

ebussieres on Jul 18, 2024 Member

done

**ebussieres** closed this as completed on Jul 18, 2024

JLLeitschuh on Jul 18, 2024 Author

Thanks!

Friendly heads up that this vulnerability disclosure follows the Open Source Security Foundation (OSSF) Model Outbound Vulnerability Disclosure Policy: Version 0.1.

JLLeitschuh on Jul 22, 2024 Author

Friendly ping, please take a look: https://github.com/PebbleTemplates/pebble/security/advisories/GHSA-7c6h-hmf9-7wj7

JLLeitschuh on Feb 23, 2025 Author

@**ebussieres** friendly heads up that the disclosure deadline has lapsed and full disclosure of the unfixed vulnerability will occur within the next week.

**JLLeitschuh** mentioned this on Feb 24, 2025

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

JLLeitschuh on Feb 28, 2025 Author

Publicly disclosed here: GHSA-p75g-cxfj-7wrx

ogomaemmanuel on Mar 24, 2025

I think pebble has loaders that can be set when configuring the engine, StringLoader,ClassLoaders, FileLoaders etc, only file loader is supposed to read from anywhere within the filesystem. You can also disallow some extensions using registerExtensionCustomizer.



## Metadata

**Assignees**

No one assigned

**Labels**

No labels

**Type**

No type

**Projects**

No projects

**Milestone**

No milestone

**Relationships**

None yet

**Development**

No branches or pull requests

**Participants**