XML Injection in the XML creator toolkit

Moderate **bastianallgeier** published **GHSA-9wfj-c55w-j9qr** 17 hours ago

Package

php **getkirby/cms** (Composer)

Affected versions

<=4.8.0, 5.0.0-5.3.3

Patched versions

4.9.0, 5.4.0

Description

TL;DR

This vulnerability only affects Kirby sites that use the `Xml` data handler (e.g. `Data::encode($string, 'xml')`) or the `Xml::create()`, `Xml::tag()` or `Xml::value()` method(s) in site or plugin code. The Kirby core does not use any of the affected methods.

If you use an affected method and cannot rule out input to these methods controlled by an attacker, we strongly recommend to update to a patch release.

Introduction

XML strings contain structured data in tags and attributes. Depending on the used XML schema, this data can carry specific meaning that can lead to actions in other systems that parse and act on the XML data. Tags and attributes are detected based on their specific syntax, which includes characters such as `<`, `>`, `"`, and `&`. If these characters are to be used verbatim in text within the XML string, they can be escaped using a `<![CDATA[ ]]>` block.

XML injection is an attack on a system generating or parsing XML files. By injecting special characters into input data, XML output with a malicious meaning could be generated by a vulnerable system.

Impact

Kirby's `Xml::value()` method has special handling for `<![CDATA[ ]]>` blocks. If the input value is already valid `CDATA`, it is not escaped a second time but allowed to pass through. However it was possible to trick this check into allowing values that only *contained* a valid `CDATA` block but also contained other structured data outside of the `CDATA` block. This structured data would then also be allowed to pass through, circumventing the value protection.

The `Xml::value()` method is used in `Xml::tag()`, `Xml::create()` and in the `Xml` data handler (e.g. `Data::encode($string, 'xml')`).

Both the vulnerable methods and the data handler are not used in the Kirby core. However they may be used in site or plugin code, e.g. to create XML strings from input data. If those generated files are passed to another implementation that assigns specific meaning to the XML schema, manipulation of this system's behavior is possible.

Kirby sites that don't use XML generation in site or plugin code are *not* affected.

Patches

The problem has been patched in Kirby 4.9.0 and Kirby 5.4.0. Please update to one of these or a later version to fix the vulnerability.

In all of the mentioned releases, we have added additional checks that only allow unchanged `CDATA` passthrough if the entire string is made up of valid `CDATA` blocks and no structured data. This protects all uses of the method against the described vulnerability.

Credits

Thanks to Patrick Falb (**@dapatrese**) at FORMER 03 for responsibly reporting the identified issue.

Severity

Moderate 6.9 / 10

CVSS v4 base metrics

Exploitability Metrics	
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	Present
Privileges Required	None
User interaction	None
Vulnerable System Impact Metrics	
Confidentiality	None
Integrity	None

Availability	None
Subsequent System Impact Metrics	
Confidentiality	None
Integrity	High
Availability	None

Learn more about base metrics

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:H/SA:N

CVE ID

CVE-2026-32870

Weaknesses

▶ CWE-91

Credits

dapatrese Finder