Potential denial of service while parsing polymorphic input with tagged polymorphism style

Moderate **charleskorn** published **GHSA-fmm9-3gv8-58f4** on Sep 5, 2021

Package

com.charleskorn.kaml:kaml (Maven)

Affected versions	Patched versions
< 0.35.2	0.35.3

Description

Impact

Attackers that could provide arbitrary YAML input to an application that uses kaml could cause the application to endlessly loop while parsing the input. This could result in resource starvation and denial of service.

This only affects applications that use polymorphic serialization with the default tagged polymorphism style. Applications using the property polymorphism style are not affected.

YAML input for a polymorphic type that provided a tag but no value for the object would trigger the issue, for example:

```
!<x>
```

The following is a sample application that demonstrates this issue:

```
import com.charleskorn.kaml.Yaml
import kotlinx.serialization.SerialName
import kotlinx.serialization.Serializable

@Serializable
private sealed class K {
    @Serializable
    @SerialName("x")
    data class X(
        val property: String? = null,
    ) : K()
}

const val s = """
!<x>
"""

fun main() {
    println("Started.")
    val result = Yaml.default.decodeFromString(K.serializer(), s)
    println("Finished, result is $result")
}
```

On vulnerable versions of kaml, the `decodeFromString()` operation hangs and never returns.

Patches

Version 0.35.3 or later contain the fix for this issue.

Workarounds

None.

References

- Original issue report: #179

For more information

If you have any questions or comments about this advisory, please start a discussion thread.

Acknowledgements

Thank you to **@ukarlsson** for reporting this issue.

Severity

Moderate **4.3** / 10

CVSS base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	None

Integrity	None
Availability	Low

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L

CVE ID

CVE-2021-39194

Weaknesses

CWE-230