Critical vulnerability found in cron-utils

Critical jmrozanec published **GHSA-pfj3-56hm-jwq5** on Nov 24, 2020

Package

com.cronutils.cron-utils (Maven)

Affected versions	Patched versions
<9.1.3	9.1.3

Description

Impact

A Template Injection was identified in cron-utils enabling attackers to inject arbitrary Java EL expressions, leading to unauthenticated Remote Code Execution (RCE) vulnerability. Versions up to 9.1.2 are susceptible to this vulnerability. Please note, that only projects using the **@Cron** annotation to validate untrusted Cron expressions are affected.

Patches

The issue was patched and a new version released. Please upgrade to version 9.1.3.

Workarounds

There are no known workarounds up to this moment.

References

A description of the issue is provided in issue 461

For more information

If you have any questions or comments about this advisory:

- Open an issue in cron-utils Github repository

Severity

Critical

CVE ID

CVE-2020-26238

Weaknesses

No CWEs

Credits

pwntester