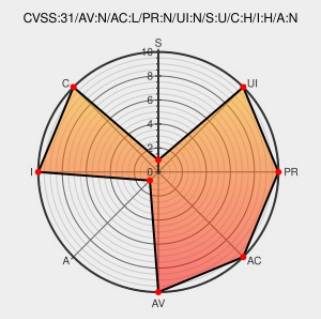
CVE-2022-41923

Published on: Not Yet Published

Last Modified on: 11/23/2022 07:15:00 PM UTC

CVE-2022-41923 - advisory for GHSA-frqg-vvxg-jqqh

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Grails-spring-security-core from Grails contain the following vulnerability:

Grails Spring Security Core plugin is vulnerable to privilege escalation. The vulnerability allows an attacker access to one endpoint (i.e. the targeted endpoint) using the authorization requirements of a different endpoint (i.e. the donor endpoint). In some Grails framework applications, access to the targeted endpoint will be granted based on meeting the authorization requirements of the donor endpoint, which can result in a privilege escalation attack. This vulnerability has been patched in grails-spring-security-core versions 3.3.2, 4.0.5 and 5.1.1. Impacted Applications: Grails Spring Security Core plugin versions: 1.x 2.x >=3.0.0 <3.3.2 >=4.0.0 <4.0.5 >=5.0.0 <5.1.1 We strongly suggest that all Grails framework applications using the Grails Spring Security Core plugin be updated to a patched release of the plugin. Workarounds: Users should create a subclass extending one of the following classes from the `grails.plugin.springsecurity.web.access.intercept` package, depending on their security configuration: * `AnnotationFilterInvocationDefinition` * `InterceptUrlMapFilterInvocationDefinition` * `RequestmapFilterInvocationDefinition` In each case, the subclass should override the `calculateUri` method like so: ``` @Override protected String calculateUri(HttpServletRequest request) { UrlPathHelper.defaultInstance.getRequestUri(request) } ``` This should be considered a temporary measure, as the patched versions of grails-spring-security-core deprecates the `calculateUri` method. Once upgraded to a patched version of the plugin, this workaround is no longer needed. The workaround is especially important for version 2.x, as no patch is available version 2.x of the GSSC plugin.

CVE-2022-41923 has been assigned by security-advisories@github.com to track the vulnerability

Affected Vendor/Software: **grails** - **grails-spring-security-core** version **>= 5.0.0, < 5.1.1**

Affected Vendor/Software: **grails** - **grails-spring-security-core** version **>= 4.0.0, < 4.0.5**

Affected Vendor/Software: **grails** - **grails-spring-security-core** version **>= 3.0.0, < 3.3.2**

Affected Vendor/Software: **grails** - **grails-spring-security-core** version **= 2.0.0**

CVE References

Description	Tags	Link
GitHub - grails/GSSC-CVE-2022-41923	github.com text/html	MISC github.com/grails/GSSC-CVE-2022-41923
Grails Spring Security Core plugin: Improper Privilege Management vulnerability · Advisory · grails/grails-spring-security-core · GitHub	github.com text/html	CONFIRM github.com/grails/grails-spring-security-core/security/advisories/GHSA-frqg-vvxg-jqqh
Grails Spring Security Core Plugin Improper Privilege Management Vulnerability	grails.org text/html	MISC grails.org/blog/2022-11-22-ss-plugin-auth-cve.html

There are currently no QIDs associated with this CVE

Known Affected Software

Vendor	Product	Version
Grails	grails-spring-security-core	>= 5.0.0, < 5.1.1
Grails	grails-spring-security-core	>= 4.0.0, < 4.0.5
Grails	grails-spring-security-core	>= 3.0.0, < 3.3.2
Grails	grails-spring-security-core	= 2.0.0

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-41923 Grails Spring Security Core plugin is vulnerable to privilege esc… twitter.com/i/web/status/1…	2022-11-23 19:56:00
/r/netcve	CVE-2022-41923	2022-11-23 19:38:12

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report