



# CVE-2022-41923

Published on: Not Yet Published

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

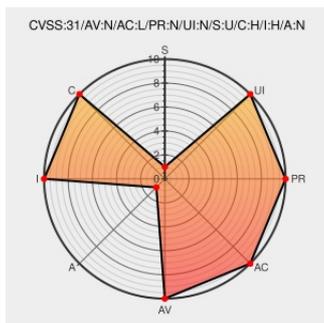
## CVE-2022-41923 - advisory for GHSA-frqg-vvxg-jqqh

[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  $\geq 3.0.0 < 3.3.2 \geq 4.0.0 < 4.0.5 \geq 5.0.0 < 5.1.1$  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) { UriPathHelper.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](mailto:security-advisories@github.com) to track the vulnerability

Affected Vendor/Software: [grails](#) - [grails-spring-security-core](#) version  $\geq 5.0.0, < 5.1.1$

Affected Vendor/Software: [grails](#) - [grails-spring-security-core](#) version  $\geq 4.0.0, < 4.0.5$

Affected Vendor/Software: [grails](#) - [grails-spring-security-core](#) version  $\geq 3.0.0, < 3.3.2$

Affected Vendor/Software: [grails](#) - [grails-spring-security-core](#) version = 2.0.0

## CVE References

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

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

## Known Affected Software

Vendor	Product	Version
Grails	<a href="#">grails-spring-security-core</a>	>= 5.0.0, < 5.1.1
Grails	<a href="#">grails-spring-security-core</a>	>= 4.0.0, < 4.0.5
Grails	<a href="#">grails-spring-security-core</a>	>= 3.0.0, < 3.3.2
Grails	<a href="#">grails-spring-security-core</a>	= 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... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2022-11-23 19:56:00
/r/netcve	<a href="#">CVE-2022-41923</a>	2022-11-23 19:38:12

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2022 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

