

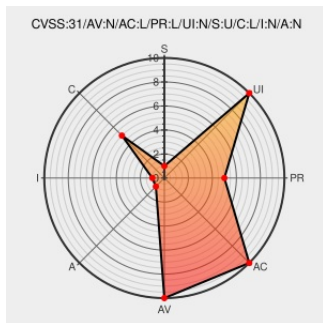


CVE-2022-23464

Published on: Not Yet Published

Last Modified on: 09/28/2022 03:39:00 PM UTC

CVE-2022-23464 - advisory for GHSL-2022-034

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Discovery](#) from [Nepxion](#) contain the following vulnerability:

Nepxion Discovery is a solution for Spring Cloud. Discovery is vulnerable to a potential Server-Side Request Forgery (SSRF). RouterResourceImpl uses RestTemplate's getForEntity to retrieve the contents of a URL containing user-controlled input, potentially resulting in Information Disclosure. There is no patch available for this issue at time of publication. There are no known workarounds.

CVE-2022-23464 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Nepxion](#) - **Discovery** version **<= 6.16.2**

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	NONE	NONE

CVE References

Description	Tags	Link
GHSL-2022-033_GHSL-2022-034: SpEL Injection in Nepxion/Discovery - CVE-2022-23463, CVE-2022-23464 GitHub Security Lab	securitylab.github.com text/html	MISC securitylab.github.com/advisories/GHSL-2022-033_GHSL-2022-034_Discovery/

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nepxion	Discovery	All	All	All	All
cpe:2.3:a:nepxion:discovery:*:*:*:*:spring_cloud:*:*						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @GHSecurityLab	GHSL-2022-033_GHSL-2022-034: SpEL Injection in Nepxion/Discovery - CVE-2022-23463, CVE-2022-23464 github.co/3Dn8dZo	2022-09-12 20:18:00
 @CVEreport	CVE-2022-23464 : Nepxion Discovery is a solution for Spring Cloud. Discovery is vulnerable to a potential Server-Si... twitter.com/i/web/status/1...	2022-09-24 04:40:56
 @LinInfoSec	Spring - CVE-2022-23464: securitylab.github.com/advisories/GHS...	2022-09-24 11:00:41
 /r/netcve	CVE-2022-23464	2022-09-24 05:38:17

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)