

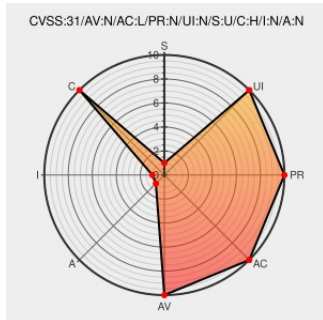


CVE-2023-2900

Published on: Not Yet Published

Last Modified on: 11/07/2023 04:13:00 AM UTC

CVE-2023-2900

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

Certain versions of [Nfine Rapid Development Platform](#) from [Nfine Rapid Development Platform Project](#) contain the following vulnerability:

A vulnerability was found in NFine Rapid Development Platform 20230511. It has been classified as problematic. Affected is an unknown function of the file /Login/CheckLogin. The manipulation leads to use of weak hash. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be

difficult. The exploit has been disclosed to the public and may be used. VDB-229974 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.

CVE-2023-2900 has been assigned by [cna@vuldb.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [NFine - Rapid Development Platform](#) version = 20230511

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
Vulnerability/NFine-Rapid-development-platform-has-weak-password-vulnerability.md at main · Peanut886/Vulnerability · GitHub	github.com text/html	MISC github.com/Peanut886/Vulnerability/blob/main/webray.com.cn/NFine-Rapid-development-platform-has-weak-password-vulnerability.md
CVE-2023-2900: NFine Rapid Development Platform CheckLogin weak hash	vuldb.com text/html	MISC vuldb.com/?id.229974

Login required

vuldb.com

text/html

Inactive Link

Not Archived

MISC vuldb.com/?ctiid.229974

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	Nfine Rapid Development Platform Project	Nfine Rapid Development Platform	2023-05-11	All	All	All
cpe:2.3:a:nfine_rapid_development_platform_project:nfine_rapid_development_platform:2023-05-11:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @fletch_ai	Fletch Top Threat Alert: Git Project Security Vulnerabilities Let Attackers Execute Arbitrary Code - #CVE-2023-2900... twitter.com/i/web/status/1...	2023-05-05 01:24:36

[← 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](#)