

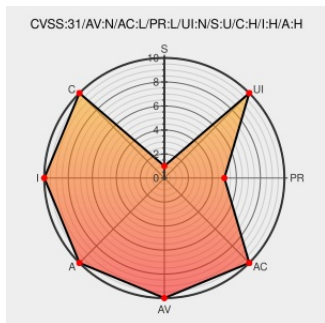


CVE-2021-4276

Published on: Not Yet Published

Last Modified on: 01/09/2023 07:57:00 PM UTC

CVE-2021-4276

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

Certain versions of [Hedgehog](#) from [Dns-stats](#) contain the following vulnerability:

A vulnerability was found in dns-stats hedgehog. It has been rated as problematic. Affected by this issue is the function

DSCIOManager::dsc_import_input_from_source of the file src/DSCIOManager.cpp. The manipulation leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to

the public and may be used. The real existence of this vulnerability is still doubted at the moment. The name of the patch is 58922c345d3d1fe89bb2020111873a3e07ca93ac. It is recommended to apply a patch to fix this issue. VDB-216746 is the identifier assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: We do assume that the Data Manager server can only be accessed by authorised users. Because of this, we don't believe this specific attack is possible without such a compromise of the Data Manager server.

CVE-2021-4276 has been assigned by [cna@vuldb.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [dns-stats](#) - [hedgehog](#) version **before 58922c345d3d1fe89bb2020111873a3e07ca93ac**

CVSS3 Score: **8.8 - HIGH**

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

CVE References

Description	Tags	Link
Merge pull request #190 from japroc/fix-potential-sqli-through-fs-	github.com text/html	MISC github.com/dns-stats/hedgehog/commit/58922c345d3d1fe89bb2020111873a3e07ca93ac

path · dns-
stats/hedgehog@58922c3 · GitHub

Fix potential sql injection through fs
path by japroc · Pull Request #190 ·
dns-stats/hedgehog · GitHub

github.com
text/html

MISC github.com/dns-stats/hedgehog/pull/190

CVE-2021-4276 | dns-stats
hedgehog DSCIOManager.cpp
dsc_import_input_from_source sql
injection (ID 190)

web.archive.org
text/html

MISC vuldb.com/?id.216746

Inactive Link Not Archived

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

Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dns-stats	Hedgehog	All	All	All	All
cpe:2.3:a:dns-stats:hedgehog:*****:*						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 /r/netcve	CVE-2021-4276	2022-12-25 11:38:17

← 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](#)