

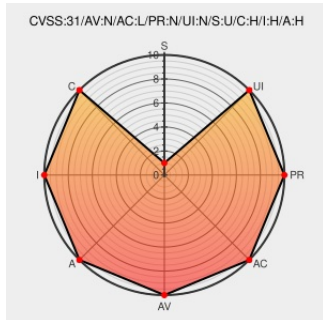


CVE-2022-36681

Published on: Not Yet Published

Last Modified on: 08/27/2022 01:27:00 AM UTC

CVE-2022-36681

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

Certain versions of [Simple Task Scheduling System](#) from [Simple Task Scheduling System Project](#) contain the following vulnerability:

Simple Task Scheduling System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /classes/Master.php?f=delete_account.

CVE-2022-36681 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector

Attack Complexity

Privileges Required

User Interaction

NETWORK

LOW

NONE

NONE

Scope

Confidentiality Impact

Integrity Impact

Availability Impact

UNCHANGED

HIGH

HIGH

HIGH

CVE References

Description

Tags

Link

bug_report/SQLi-5.md at main · k0xx11/bug_report · GitHub

[github.com](#)
[text/html](#)

[MISC github.com/k0xx11/bug_report/blob/main/vendors/oretnom23/simple-task-scheduler-system/SQLi-5.md](#)

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

Simple Task Scheduling System v1.0 was discovered to contain a SQL injection vulnerability

Simple Task Scheduling System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /c...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Simple Task Scheduling System Project	Simple Task Scheduling System	1.0	All	All	All

cpe:2.3:a:simple_task_scheduling_system_project:simple_task_scheduling_system:1.0:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-36681 : Simple Task Scheduling System v1.0 was discovered to contain a SQL injection vulnerability via the... twitter.com/i/web/status/1...	2022-08-26 13:06:09
 @Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-36681 Simple Task Scheduling System v1.0 was discovered to contain a SQ... twitter.com/i/web/status/1...	2022-08-26 14:56:00
 @LinInfoSec	Php - CVE-2022-36681: github.com/k0xx11/bug_rep...	2022-08-26 15:00:05
 @threatmeter	CVE-2022-36681 Simple Task Scheduling System v1.0 was discovered to contain a SQL injection vulnerability via the i... twitter.com/i/web/status/1...	2022-08-26 23:25:59
 @ColorTokensInc	Emerging Vulnerability Found CVE-2022-36681 - Simple Task Scheduling System v1.0 was discovered to contain a SQL in... twitter.com/i/web/status/1...	2022-08-27 01:42:17
 @threatmeter	CVE-2022-36681 Simple Task Scheduling System v1.0 was discovered to contain a SQL injection vulnerability via the i... twitter.com/i/web/status/1...	2022-08-28 07:09:53
 /r/netcve	CVE-2022-36681	2022-08-26 13:38:44

[← 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](#)