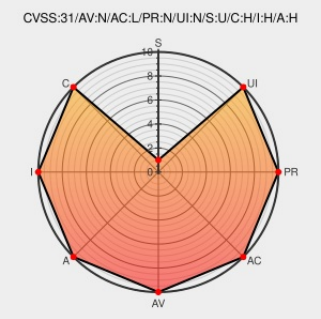
# CVE-2021-27886

Published on: 03/01/2021 12:00:00 AM UTC

Last Modified on: 05/23/2022 03:59:00 PM UTC

## CVE-2021-27886

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Docker Dashboard from Docker Dashboard Project contain the following vulnerability:

rakibtg Docker Dashboard before 2021-02-28 allows command injection in backend/utilities/terminal.js via shell metacharacters in the command parameter of an API request. NOTE: this is NOT a Docker, Inc. product.

CVE-2021-27886 has been assigned by 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 |

### CVSS2 Score: 7.5 - HIGH

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | LOW | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| PARTIAL | PARTIAL | PARTIAL |

### CVE References

| Description | Tags | Link |
|---|---|---|
| Docker Dashboard Remote Command Execution ≈ Packet Storm | packetstormsecurity.com text/html | MISC packetstormsecurity.com/files/163416/Docker-Dashboard-Remote-Command-Execution.html |
| Docker Legal Terms | Third Party Advisory www.docker.com | MISC www.docker.com/legal/trademark-guidelines |

| | | |
|---|---|---|
| | text/html | |
| Security: lack of input validation in APIs leads to command injection · Issue #23 · rakibtg/docker-web-gui · GitHub | Third Party Advisory<br>github.com<br>text/html | MISC github.com/rakibtg/docker-web-gui/issues/23 |
| Fixed security issue with terminal by introducing controlled method t… · rakibtg/docker-web-gui@79cdc41 · GitHub | Patch<br>Third Party Advisory<br>github.com<br>text/html | MISC github.com/rakibtg/docker-web-gui/commit/79cdc41809f2030fce21a1109898bd79e4190661 |

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 | Docker Dashboard Project | Docker Dashboard | All | All | All | All |
| Application | Docker Dashboard Project | Docker Dashboard | All | All | All | All |

cpe:2.3:a:docker_dashboard_project:docker_dashboard:*:*:*:*:*:*:*:*:

cpe:2.3:a:docker_dashboard_project:docker_dashboard:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

## Social Mentions

| Source | Title | Posted (UTC) |
|---|---|---|
| @LinInfoSec | Docker - CVE-2021-27886: github.com/rakibtg/docker… | 2022-05-23 17:02:00 |

← Previous ID

Next ID→