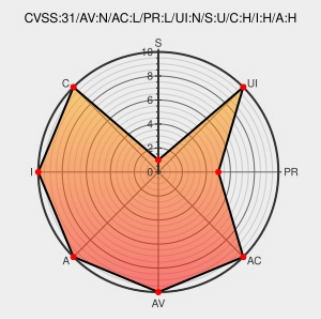
CVE-2021-31590

Published on: 07/19/2021 12:00:00 AM UTC

Last Modified on: 07/12/2022 05:42:00 PM UTC

CVE-2021-31590

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



Certain versions of Pwndoc from Pwndoc Project contain the following vulnerability:

PwnDoc all versions until 0.4.0 (2021-08-23) has incorrect JSON Webtoken handling, leading to incorrect access control. With a valid JSON Webtoken that is used for authentication and authorization, a user can keep his admin privileges even if he is downgraded to the "user" privilege. Even after a user's account is deleted, the user can still access the administration panel (and add or delete users) and has complete access to the system.

CVE-2021-31590 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

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

CVSS2 Score: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Security Advisories · pwndoc/pwndoc · GitHub		MISC github.com/pwndoc/pwndoc/security/advisories

Security Advisories · pwndoc/pwndoc · GitHub	github.com text/html	MISC github.com/pwndoc/pwndoc/security/advisories
pwndoc/CHANGELOG.md at 59519735b0d831d8fd96d7c3387f66d28407e583 · pwndoc/pwndoc · GitHub	github.com text/html	MISC github.com/pwndoc/pwndoc/blob/59519735b0d831d8fd96d7c3387f66d284 2021-08-23
Update JWT generation · pwndoc/pwndoc@15f3dc0 · GitHub	github.com text/html	MISC github.com/pwndoc/pwndoc/commit/15f3dc0e212eda465e05fda0
Applied fix for CVE-2021-31590 by Lednerb · Pull Request #128 · pwndoc/pwndoc · GitHub	github.com text/html	MISC github.com/pwndoc/pwndoc/pull/128
Update Session management using refresh token · pwndoc/pwndoc@ff1b868 · GitHub	github.com text/html	MISC github.com/pwndoc/pwndoc/commit/ff1b868cec55f5b6c7a91e15a
DGC | Deutsche Gesellschaft für Cybersicherheit | PwnDoc - Incorrect Access Control Vulnerability	www.dgc.org text/html	MISC www.dgc.org/responsible_disclosure_pwndoc_jwt
Security Update: Change JWT Secret and TLS Certificate automatically on build by Lednerb · Pull Request #74 · pwndoc/pwndoc · GitHub	github.com text/html	MISC github.com/pwndoc/pwndoc/pull/74

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	Pwndoc Project	Pwndoc	All	All	All	All
Application	Pwndoc Project	Pwndoc	All	All	All	All

cpe:2.3:a:pwndoc_project:pwndoc:*:*:*:*:*:*:*:*:

cpe:2.3:a:pwndoc_project:pwndoc:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-31590 : PwnDoc through 2021-04-22 has incorrect JSON Webtoken handling, leading to incorrect access contro… twitter.com/i/web/status/1…	2021-07-19 20:04:51
@SecRiskRptSME	RT: CVE-2021-31590 PwnDoc through 2021-04-22 has incorrect JSON Webtoken handling, leading to incorrect access con… twitter.com/i/web/status/1…	2021-07-20 07:21:24
/r/netcve	CVE-2021-31590	2021-07-19 20:40:43

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report