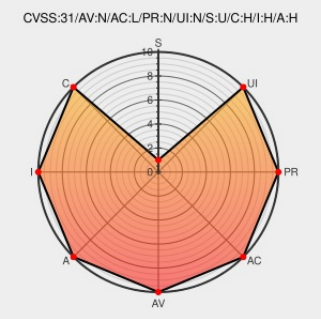
CVE-2020-10539

Published on: 02/05/2021 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-10539

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



Certain versions of Epikur from Epikur contain the following vulnerability:

An issue was discovered in Epikur before 20.1.1. The Epikur server contains the checkPasswort() function that, upon user login, checks the submitted password against the user password's MD5 hash stored in the database. It is also compared to a second MD5 hash, which is the same for every user (aka a "Backdoor Password" of 3p1kursupport). If the submitted password matches either one, access is granted.

CVE-2020-10539 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
Advisory X41-2020-003: Multiple Vulnerabilities in Epikur | X41 D-SEC GmbH	Exploit, Third Party Advisory	MISC www.x41-dsec.de/lab/advisories/x41-2020-003-epikur

www.x41-dsec.de
text/html

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	Epikur	Epikur	All	All	All	All
Application	Epikur	Epikur	All	All	All	All

cpe:2.3:a:epikur:epikur:*:*:*:*:*:*:*:*:

cpe:2.3:a:epikur:epikur:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→