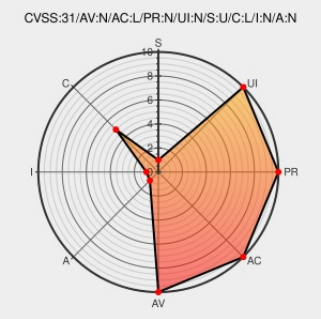
CVE-2020-15392

Published on: 07/07/2020 12:00:00 AM UTC

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

CVE-2020-15392

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



Certain versions of Supravizio Bpm from Venki contain the following vulnerability:

A user enumeration vulnerability flaw was found in Venki Supravizio BPM 10.1.2. This issue occurs during password recovery, where a difference in error messages could allow an attacker to determine if a username is valid or not, enabling a brute-force attack with valid usernames.

CVE-2020-15392 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.3 - MEDIUM

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Venki Tecnologia em Software	Vendor Advisory www.venki.com.br text/html	MISC www.venki.com.br/

GitHub - inflixim4be/CVE-2020-15392: User Enumeration on Supravizio BPM 10.1.2

Exploit
Third Party Advisory
github.com
text/html

MISC github.com/inflixim4be/CVE-2020-15392

There are currently no QIDs associated with this CVE

Exploit/POC from Github

User Enumeration on Supravizio BPM 10.1.2

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Venki	Supravizio Bpm	10.1.2	All	All	All
Application	Venki	Supravizio Bpm	10.1.2	All	All	All

cpe:2.3:a:venki:supravizio_bpm:10.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:venki:supravizio_bpm:10.1.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→