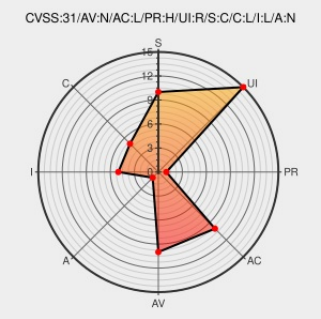
CVE-2023-3196

Published on: Not Yet Published

Last Modified on: 10/05/2023 12:56:00 AM UTC

CVE-2023-3196

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



Certain versions of Canopsis from Capensis contain the following vulnerability:

This vulnerability could allow an attacker to store a malicious JavaScript payload in the login footer and login page description parameters within the administration panel.

CVE-2023-3196 has been assigned by cve-coordination@incibe.es to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Capensis** - **Canopsis** version **= 23.04-alpha3**

CVSS3 Score: 4.8 - MEDIUM

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

CVE References

Description	Tags	Link
Multiple Vulnerabilities Canopsis Capensis | INCIBE-CERT | INCIBE	www.incibe.es text/html	MISC www.incibe.es/en/incibe-cert/notices/aviso/multiple-vulnerabilities-canopsis-capensis

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Capensis	Canopsis	23.04	alpha3	All	All

cpe:2.3:a:capensis:canopsis:23.04:alpha3:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→