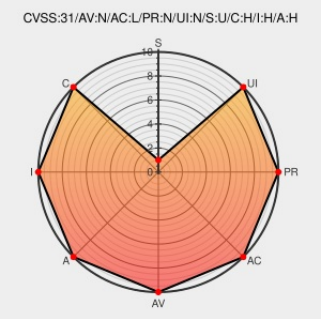
CVE-2020-20269

Published on: 01/22/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:53 PM UTC

CVE-2020-20269

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



Certain versions of Caret from Caret contain the following vulnerability:

A specially crafted Markdown document could cause the execution of malicious JavaScript code in Caret Editor before 4.0.0-rc22.

CVE-2020-20269 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: 10 - HIGH

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

CVE References

Description	Tags	Link
Release 4.0.0-rc22 · careteditor/releases-beta · GitHub	Release Notes Third Party Advisory github.com text/html	MISC github.com/careteditor/releases-beta/releases/tag/4.0.0-rc22

caret.io - Registered at Namecheap.com	Product caret.io text/html	MISC caret.io
Full Disclosure: CVE-2020-20269 - Caret Editor v4.0.0-rc21 Remote Code Execution	Mailing List Third Party Advisory seclists.org text/html	FULLDISC 20210122 CVE-2020-20269 - Caret Editor v4.0.0-rc21 Remote Code Execution
Caret Editor 4.0.0-rc21 Remote Code Execution ≈ Packet Storm	Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/161072/Caret-Editor-4.0.0-rc21-Remote-Code-Execution.html
Critical security vulnerability in Caret 4.0.0-rc21 · Issue #841 · careteditor/issues · GitHub	Issue Tracking Third Party Advisory github.com text/html	MISC github.com/careteditor/issues/issues/841
Full Disclosure: CVE-2020-20269 - Caret Editor v4.0.0-rc21 Remote Code Execution	Mailing List Third Party Advisory seclists.org text/html	MISC seclists.org/fulldisclosure/2021/Jan/59

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Caret	Caret	4.0.0	beta0	All	All
Application	Caret	Caret	4.0.0	beta1	All	All
Application	Caret	Caret	4.0.0	beta2	All	All
Application	Caret	Caret	4.0.0	beta3	All	All
Application	Caret	Caret	4.0.0	beta4	All	All
Application	Caret	Caret	4.0.0	beta5	All	All
Application	Caret	Caret	4.0.0	beta6	All	All
Application	Caret	Caret	4.0.0	beta7	All	All
Application	Caret	Caret	4.0.0	beta8	All	All
Application	Caret	Caret	4.0.0	beta9	All	All
Application	Caret	Caret	4.0.0	rc1	All	All
Application	Caret	Caret	4.0.0	rc10	All	All
Application	Caret	Caret	4.0.0	rc11	All	All
Application	Caret	Caret	4.0.0	rc12	All	All
Application	Caret	Caret	4.0.0	rc13	All	All

Application	Caret	Caret	4.0.0	rc14	All	All
Application	Caret	Caret	4.0.0	rc15	All	All
Application	Caret	Caret	4.0.0	rc16	All	All
Application	Caret	Caret	4.0.0	rc17	All	All
Application	Caret	Caret	4.0.0	rc18	All	All
Application	Caret	Caret	4.0.0	rc19	All	All
Application	Caret	Caret	4.0.0	rc2	All	All
Application	Caret	Caret	4.0.0	rc20	All	All
Application	Caret	Caret	4.0.0	rc21	All	All
Application	Caret	Caret	4.0.0	beta0	All	All
Application	Caret	Caret	4.0.0	beta1	All	All
Application	Caret	Caret	4.0.0	beta2	All	All
Application	Caret	Caret	4.0.0	beta3	All	All
Application	Caret	Caret	4.0.0	beta4	All	All
Application	Caret	Caret	4.0.0	beta5	All	All
Application	Caret	Caret	4.0.0	beta6	All	All
Application	Caret	Caret	4.0.0	beta7	All	All
Application	Caret	Caret	4.0.0	beta8	All	All
Application	Caret	Caret	4.0.0	beta9	All	All
Application	Caret	Caret	4.0.0	rc1	All	All
Application	Caret	Caret	4.0.0	rc10	All	All
Application	Caret	Caret	4.0.0	rc11	All	All
Application	Caret	Caret	4.0.0	rc12	All	All
Application	Caret	Caret	4.0.0	rc13	All	All
Application	Caret	Caret	4.0.0	rc14	All	All
Application	Caret	Caret	4.0.0	rc15	All	All
Application	Caret	Caret	4.0.0	rc16	All	All
Application	Caret	Caret	4.0.0	rc17	All	All
Application	Caret	Caret	4.0.0	rc18	All	All
Application	Caret	Caret	4.0.0	rc19	All	All
Application	Caret	Caret	4.0.0	rc2	All	All
Application	Caret	Caret	4.0.0	rc20	All	All
Application	Caret	Caret	4.0.0	rc21	All	All
Application	Caret	Caret	All	All	All	All

cpe:2.3:a:caret:caret:4.0.0:beta0:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:beta1:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:beta2:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:beta3:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:beta4:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:beta5:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:beta6:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:beta7:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:beta8:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:beta9:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:rc10:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:rc11:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:rc12:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:rc13:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:rc14:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:rc15:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:rc16:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:rc17:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:rc18:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:rc19:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:rc20:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:rc21:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:beta0:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:beta1:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:beta2:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:beta3:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:beta4:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:beta5:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:beta6:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:beta7:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:beta8:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:beta9:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:rc10:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:rc11:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:rc12:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:rc13:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:rc14:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:rc15:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:rc16:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:rc17:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:rc18:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:rc19:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:rc20:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:4.0.0:rc21:*:*:*:*:*:*:

cpe:2.3:a:caret:caret:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→