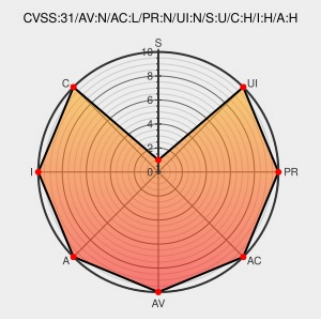
CVE-2020-7640

Published on: 04/27/2020 12:00:00 AM UTC

Last Modified on: 11/07/2023 03:26:00 AM UTC

CVE-2020-7640

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



Certain versions of Pixl-class from Pixlcore contain the following vulnerability:

pixl-class prior to 1.0.3 allows execution of arbitrary commands. The members argument of the create function can be controlled by users without any sanitization.

CVE-2020-7640 has been assigned by report@snyk.io 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
Version 1.0.3 · jhuckaby/pixl-class@47677a3 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/jhuckaby/pixl-class/commit/47677a3638e3583e42f3a05cc7f0b30293d2acc8

Arbitrary Code Execution in pixl-class | Snyk	Patch Third Party Advisory snyk.io text/html	MISC snyk.io/vuln/SNYK-JS-PIXLCLASS-564968
	Broken Link github.com text/plain Inactive Link Not Archived	MISC github.com/jhuckaby/pixl-class/commit/47677a3638e3583e42f3a05cc7f0b30293d2acc8,

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pixlcore	Pixl-class	All	All	All	All
Application	Pixlcore	Pixl-class	All	All	All	All

cpe:2.3:a:pixlcore:pixl-class:*:*:*:*:*:node.js:*:*:

cpe:2.3:a:pixlcore:pixl-class:*:*:*:*:*:node.js:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→