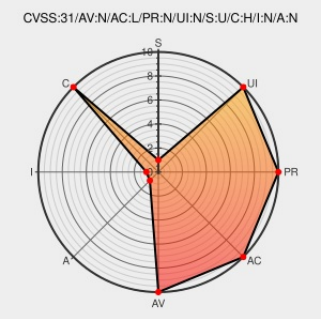
CVE-2018-7166

Published on: 08/21/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:39 PM UTC

CVE-2018-7166

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



Certain versions of Node.js from Nodejs contain the following vulnerability:

In all versions of Node.js 10 prior to 10.9.0, an argument processing flaw can cause `Buffer.alloc()` to return uninitialized memory. This method is intended to be safe and only return initialized, or cleared, memory. The third argument specifying `encoding` can be passed as a number, this is misinterpreted by `Buffer's` internal "fill" method as the `start` to a fill operation. This flaw may be abused where `Buffer.alloc()` arguments are derived from user input to return uncleared memory blocks that may contain sensitive information.

CVE-2018-7166 has been assigned by cve-request@iojs.org to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **The Node.js Project** - **Node.js** version **All versions of Node.js 10 prior to 10.9.0**

CVSS3 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2018:2553
August 2018 Security Releases | Node.js	Vendor Advisory nodejs.org text/html	CONFIRM nodejs.org/en/blog/vulnerability/august-2018-security-releases/

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	Nodejs	Node.js	All	All	All	All
Application	Nodejs	Node.js	All	All	All	All

cpe:2.3:a:nodejs:node.js:*:*:*:*:*:*:*:*:

cpe:2.3:a:nodejs:node.js:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→