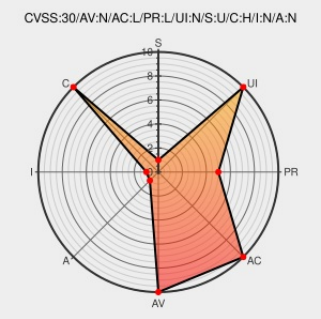
CVE-2017-16024

Published on: 06/04/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:38 PM UTC

CVE-2017-16024

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



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

The sync-exec module is used to simulate child_process.execSync in node versions <0.11.9. Sync-exec uses tmp directories as a buffer before returning values. Other users on the server have read access to the tmp directory, possibly allowing an attacker on the server to obtain confidential information from the buffer/tmp file, while it exists.

CVE-2017-16024 has been assigned by support@hackerone.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **HackerOne** - **sync-exec node module** version **All versions**

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
Insecure temporary directores · Issue #17 · gvarsanyi/sync-	Issue Tracking	MISC github.com/gvarsanyi/sync-exec/issues/17

exec · GitHub	Third Party Advisory github.com text/html	
Insecure Temporary File - OWASP	Third Party Advisory www.owasp.org text/html	MISC www.owasp.org/index.php/Insecure_Temporary_File
CWE - Individual CWE Dictionary Definition (Draft 6)	Third Party Advisory cwe.mitre.org text/html	MISC cwe.mitre.org/data/definitions/377.html
Overview	Third Party Advisory nodesecurity.io text/html	MISC nodesecurity.io/advisories/310

Related QID Numbers

983421 Nodejs (npm) Security Update for sync-exec (GHSA-38h8-x697-gh8q)

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
Application	Sync-exec Project	Sync-exec	All	All	All	All

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

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

cpe:2.3:a:sync-exec_project:sync-exec:*:*:*:*:*:node.js:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→