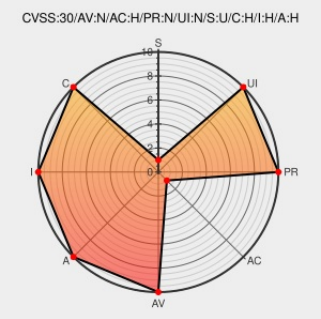
CVE-2016-10679

Published on: 05/29/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:00 PM UTC

CVE-2016-10679

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



Certain versions of Selenium-standalone-painful from Selenium-standalone-painful Project contain the following vulnerability:

selenium-standalone-painful installs a start-selenium command line to start a standalone selenium server with chrome-driver. selenium-standalone-painful downloads binary resources over HTTP, which leaves it vulnerable to MITM attacks. It may be possible to cause remote code execution (RCE) by swapping out the requested resources with an attacker controlled copy if the attacker is on the network or positioned in between the user and the remote server.

CVE-2016-10679 has been assigned by support@hackerone.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **HackerOne** - **selenium-standalone-painful node module** version **All versions**

CVSS3 Score: 8.1 - HIGH

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

CVSS2 Score: 9.3 - HIGH

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

CVE References

Description	Tags	Link
Overview	Third Party Advisory nodesecurity.io text/html	MISC nodesecurity.io/advisories/284

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.

Related QID Numbers

983432 Nodejs (npm) Security Update for selenium-standalone-painful (GHSA-3x83-p476-vv95)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Selenium-standalone-painful Project	Selenium-standalone-painful	All	All	All	All

cpe:2.3:a:selenium-standalone-painful_project:selenium-standalone-painful:*:*:*:*:*:node.js:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→