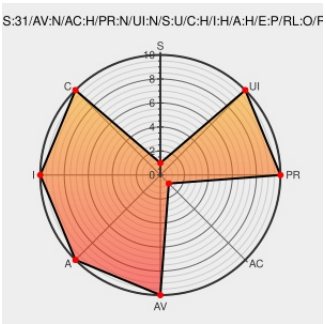
CVE-2020-28502

Published on: 03/05/2021 12:00:00 AM UTC

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

CVE-2020-28502

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



Certain versions of Xmlhttprequest from Xmlhttprequest Project contain the following vulnerability:

This affects the package xmlhttprequest before 1.7.0; all versions of package xmlhttprequest-ssl. Provided requests are sent synchronously (async=False on xhr.open), malicious user input flowing into xhr.send could result in arbitrary code being injected and run.

CVE-2020-28502 has been assigned by report@snyk.io to track the vulnerability - currently rated as HIGH severity.

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: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
Arbitrary Code Injection in org.webjars.npm:xmlhttprequest-ssl | Snyk	Exploit, Third Party Advisory, snyk.io, text/html	MISC snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1082937

Arbitrary Code Injection in org.webjars.npm:xmlhttprequest | Snyk	Exploit Third Party Advisory snyk.io text/html	MISC snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1082938
node-XMLHttpRequest/XMLHttpRequest.js at 1.6.0 · driverdan/node-XMLHttpRequest · GitHub	Broken Link github.com text/html	MISC github.com/driverdan/node-XMLHttpRequest/blob/1.6.0/lib/XMLHttpRequest.js%23L480
Arbitrary Code Injection in xmlhttprequest-ssl | Snyk	Exploit Third Party Advisory snyk.io text/html	MISC snyk.io/vuln/SNYK-JS-XMLHTTPREQUESTSSL-1082936
Arbitrary Code Injection in xmlhttprequest | Snyk	Exploit Third Party Advisory snyk.io text/html	MISC snyk.io/vuln/SNYK-JS-XMLHTTPREQUEST-1082935

Related QID Numbers

982688 Nodejs (npm) Security Update for xmlhttprequest-ssl (GHSA-h4j5-c7cj-74xg)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xmlhttprequest Project	Xmlhttprequest	All	All	All	All
Application	Xmlhttprequest Project	Xmlhttprequest	All	All	All	All

cpe:2.3:a:xmlhttprequest_project:xmlhttprequest:*:*:*:*:*:node.js:*:*

cpe:2.3:a:xmlhttprequest_project:xmlhttprequest:*:*:*:*:*:node.js:*:*

Discovery Credit

rinsuki

Social Mentions

Source	Title	Posted (UTC)
@prenone1	So CVE-2020-28502 happened. Setting a up a secure network for my servers using #iptables?	2021-05-12 13:42:49
@AlirezaGhahrood	exploit CVE-2020-28502: node-XMLHttpRequest RCE lnkd.in/d2s6vx7 Seed Selection for Successful Fuzzing… twitter.com/i/web/status/1…	2021-05-15 02:32:39
@azu_re	見てる: "Fix CVE-2020-28502 · mjwwit/node-XMLHttpRequest@ee1e81f" github.com/mjwwit/node-XM…	2021-06-26 15:50:56

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report