



CVE-2017-16129

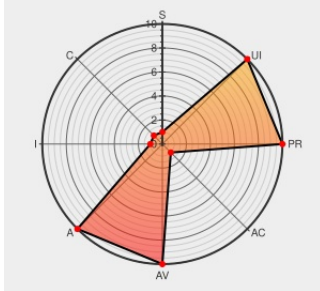
Published on: 06/06/2018 12:00:00 AM UTC

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

CVE-2017-16129

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H



Certain versions of [Superagent](#) from [Superagent Project](#) contain the following vulnerability:

The HTTP client module superagent is vulnerable to ZIP bomb attacks. In a ZIP bomb attack, the HTTP server replies with a compressed response that becomes several magnitudes larger once uncompressed. If a client does not take special care when processing such responses, it may result in excessive CPU and/or memory

consumption. An attacker might exploit such a weakness for a DoS attack. To exploit this the attacker must control the location (URL) that superagent makes a request to.

CVE-2017-16129 has been assigned by [h1](#) support@hackerone.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [h1](#) **HackerOne** - **superagent node module** version <3.7.0

CVSS3 Score: **5.9 - MEDIUM**

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

CVSS2 Score: **7.1 - HIGH**

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

CVE References

Description

Limit maximum response size · Issue #1259 · visionmedia/superagent · GitHub

Tags

Issue Tracking

Patch

Third Party Advisory

github.com

text/html

Link

MISC

github.com/visionmedia/superagent/issues/1259

Description

Node Security Platform | Advisory

Tags

Third Party Advisory

nodesecurity.io

text/html

Link

S MISC

nodesecurity.io/advisories/479

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

983904 Nodejs (npm) Security Update for superagent (GHSA-8225-6cvr-8ppq)

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:superagent_project:superagent:*.***.***:node.js:*.**:

cpe:2.3:a:superagent_project:superagent:*.***.***:node.js:*.**:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →