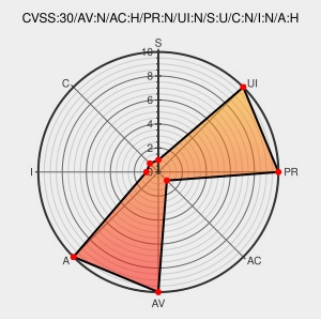
CVE-2017-16129

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



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 support@hackerone.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **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	Tags	Link
Limit maximum response size · Issue #1259 · visionmedia/superagent · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	MISC github.com/visionmedia/superagent/issues/1259
Node Security Platform | Advisory	Third Party Advisory nodesecurity.io text/html	MISC nodesecurity.io/advisories/479

Related QID Numbers

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

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→