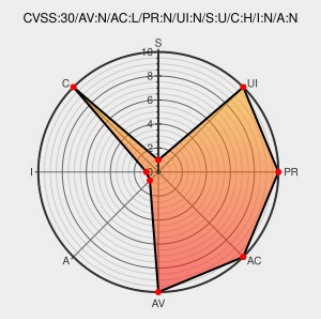
CVE-2017-16089

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

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

CVE-2017-16089

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



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

serverlyr is a simple http server. serverlyr is vulnerable to a directory traversal issue, giving an attacker access to the filesystem by placing "../" in the URL.

CVE-2017-16089 has been assigned by support@hackerone.com to track the vulnerability - currently rated as HIGH severity.

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

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
NPM-Vuln-PoC/directory-traversal/serverlyr at master · JacksonGL/NPM-Vuln-PoC · GitHub	Exploit, Third Party Advisory, github.com	MISC github.com/JacksonGL/NPM-Vuln-PoC/tree/master/directory-traversal/serverlyr

	text/html	
Overview	Exploit Third Party Advisory nodesecurity.io text/html	MISC nodesecurity.io/advisories/365

Related QID Numbers

983012 Nodejs (npm) Security Update for serverlyr (GHSA-46q2-93hm-52p5)

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:serverlyr_project:serverlyr:*:*:*:*:*:node.js:*:*:

cpe:2.3:a:serverlyr_project:serverlyr:*:*:*:*:*:node.js:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→