

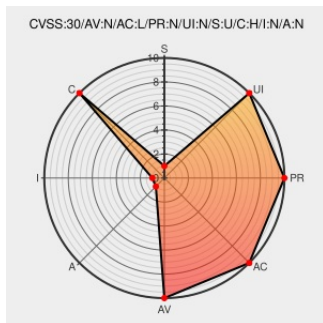


CVE-2017-16153

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

Last Modified on: 03/23/2021 11:26:39 PM UTC

CVE-2017-16153

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

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

gaoxuyan is vulnerable to a directory traversal issue, giving an attacker access to the filesystem by placing "../" in the url.

CVE-2017-16153 has been assigned by [HackerOne](#) support@hackerone.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [HackerOne](#) - **gaoxuyan 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
Overview	Vendor Advisory nodesecurity.io text/html	S MISC nodesecurity.io/advisories/378

MISC github.com/JacksonGL/NPM-Vuln-PoC/tree/master/directory-traversal/gaoxuyan

Related QID Numbers

Known Affected Configurations (CPE V2.3)

No vendor comments have been submitted for this CVE

Next ID→