



CVE-2021-23354

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2021-23354
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-12 15:15:00 UTC
Updated	2023-08-08 14:22:00 UTC
Description	The package printf before 0.6.1 are vulnerable to Regular Expression Denial of Service (ReDoS) via the regex string ^%{?'

Risk And Classification

Problem Types: CWE-1333

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Adaltas	Printf	All	All	All	All

References

Reference	Source	Link	Tags
Regular Expression Denial of Service (ReDoS) in printf Snyk	CONFIRM	snyk.io	Broken Link
ReDoS in printf · Issue #31 · adaltas/node-printf · GitHub	CONFIRM	github.com	Exploit, Issue Tracking, Third Party Advisory
Fix ReDoS by yetingli · Pull Request #32 · adaltas/node-printf · GitHub	CONFIRM	github.com	Patch, Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: Yeting Li

Legacy QID Mappings

[982885](#) Nodejs (npm) Security Update for printf (GHSA-xfhp-gmh8-r8v2)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)