



CVE-2018-20801

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

Summary

CVE	CVE-2018-20801
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-14 16:29:00 UTC
Updated	2019-07-15 11:15:00 UTC
Description	In js/parts/SvgRenderer.js in Highcharts JS before 6.1.0, the use of backtracking regular expressions permitted an attacker

Risk And Classification

Problem Types: CWE-185

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Highcharts	Highcharts	All	All	All	All
Application	Highcharts	Highcharts	All	All	All	All

References

Reference	Source	Link
CVE-2018-20801 Highcharts Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security
Regular Expression Denial of Service (ReDoS) in highcharts Snyk	MISC	snyk.io
Refactored SVGRenderer text to not use backtracking regexes to replac... · highcharts/highcharts@7c547e1 · GitHub	MISC	github.c
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

980787 Nodejs (npm) Security Update for highcharts (GHSA-xmc8-cjfr-phx3)

© [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](#)