



# CVE-2021-27290

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

## Summary

<b>CVE</b>	CVE-2021-27290
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-03-12 22:15:00 UTC
<b>Updated</b>	2022-05-13 20:51:00 UTC
<b>Description</b>	ssri 5.2.2-8.0.0, fixed in 8.0.1, processes SRIs using a regular expression which is vulnerable to a denial of service. Malicious

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Oracle</a>	<a href="#">Graalvm</a>	20.3.3	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Graalvm</a>	21.2.0	All	All	All
Application	<a href="#">Siemens</a>	<a href="#">Sinec Infrastructure Network Services</a>	All	All	All	All
Application	<a href="#">Ssri Project</a>	<a href="#">Ssri</a>	All	All	All	All

## References

Reference	Source	Link	Tags
<a href="https://doyensec.com/resources/Doyensec_Advisory_ssri_redos.pdf">doyensec.com/resources/Doyensec_Advisory_ssri_redos.pdf</a>	MISC	<a href="https://doyensec.com">doyensec.com</a>	Exploit, Patch, Third Party Advisory
Oracle Critical Patch Update Advisory - October 2021	MISC	<a href="https://www.oracle.com">www.oracle.com</a>	
<a href="https://cert-portal.siemens.com/productcert/pdf/ssa-389290.pdf">cert-portal.siemens.com/productcert/pdf/ssa-389290.pdf</a>	CONFIRM	<a href="https://cert-portal.siemens.com">cert-portal.siemens.com</a>	
SaveResults/ssri-redos.pdf at main · yetingli/SaveResults · GitHub	MISC	<a href="https://github.com">github.com</a>	Exploit, Third Party Advisory
parked	MISC	<a href="https://npmjs.com">npmjs.com</a>	Product
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[159345](#) Oracle Enterprise Linux Security Update for nodejs:12 (ELSA-2021-3073)

[159346](#) Oracle Enterprise Linux Security Update for nodejs:14 (ELSA-2021-3074)

[180031](#) Debian Security Update for node-ssri (CVE-2021-27290)

[239531](#) Red Hat Update for rh-nodejs14-nodejs and rh-nodejs14-nodejs-nodemon (RHSA-2021:2932)

[239532](#) Red Hat Update for rh-nodejs12-nodejs and rh-nodejs12-nodejs-nodemon (RHSA-2021:2931)

[239547](#) Red Hat Update for nodejs:14 (RHSA-2021:3074)

[239548](#) Red Hat Update for nodejs:12 (RHSA-2021:3073)

[239654](#) Red Hat Update for nodejs:12 (RHSA-2021:3639)

[239655](#) Red Hat Update for nodejs:12 (RHSA-2021:3638)

[375692](#) Node.js Denial Of Service and PATH,DLL hijacking Vulnerabilities July 2021

[376087](#) Azul Java Multiple Vulnerabilities Security Update October 2021

[377329](#) Alibaba Cloud Linux Security Update for nodejs:14 (ALINUX3-SA-2021:0056)

[501450](#) Alpine Linux Security Update for nodejs

[690034](#) Free Berkeley Software Distribution (FreeBSD) Security Update for node.js (c174118e-1b11-11ec-9d9d-0022489ad614)

[750833](#) OpenSUSE Security Update for nodejs12 (openSUSE-SU-2021:2327-1)

[750837](#) SUSE Enterprise Linux Security Update for nodejs10 (SUSE-SU-2021:2353-1)

[750840](#) OpenSUSE Security Update for nodejs10 (openSUSE-SU-2021:2353-1)

[750841](#) OpenSUSE Security Update for nodejs14 (openSUSE-SU-2021:2354-1)

[750857](#) OpenSUSE Security Update for nodejs14 (openSUSE-SU-2021:1060-1)

[750858](#) OpenSUSE Security Update for nodejs10 (openSUSE-SU-2021:1061-1)

[750859](#) OpenSUSE Security Update for nodejs12 (openSUSE-SU-2021:1059-1)

[750922](#) SUSE Enterprise Linux Security Update for nodejs8 (SUSE-SU-2021:2620-1)

[750928](#) OpenSUSE Security Update for nodejs8 (openSUSE-SU-2021:2618-1)

[750939](#) OpenSUSE Security Update for nodejs8 (openSUSE-SU-2021:1113-1)

[940245](#) AlmaLinux Security Update for nodejs:14 (ALSA-2021:3074)

[940398](#) AlmaLinux Security Update for nodejs:12 (ALSA-2021:3073)

[960063](#) Rocky Linux Security Update for nodejs:14 (RLSA-2021:3074)

[960082](#) Rocky Linux Security Update for nodejs:12 (RLSA-2021:3073)

© [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](#).

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