



# CVE-2021-43519

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

## Summary

<b>CVE</b>	CVE-2021-43519
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-11-09 13:15:00 UTC
<b>Updated</b>	2023-11-07 03:39:00 UTC
<b>Description</b>	Stack overflow in lua_resume of ldo.c in Lua Interpreter 5.1.0~5.4.4 allows attackers to perform a Denial of Service via a cr

## Risk And Classification

**Problem Types:** CWE-674

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	35	All	All	All
Application	<a href="#">Lua</a>	<a href="#">Lua</a>	All	All	All	All
Application	<a href="#">Lua</a>	<a href="#">Lua</a>	All	All	All	All

## References

Reference	Source	Link	Tags
[SECURITY] Fedora 35 Update: lua-5.4.4-1.fc35 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
Crash: Recursive coroutine with pcall leads to stackoverflow of interpreter	MISC	<a href="https://lua-users.org">lua-users.org</a>	
[SECURITY] Fedora 34 Update: lua-5.4.4-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 35 Update: lua-5.4.4-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 34 Update: lua-5.4.4-1.fc34 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
Re: Crash: Recursive coroutine with pcall leads to stackoverflow of interpreter	MISC	<a href="https://lua-users.org">lua-users.org</a>	
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

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">160489</a> Oracle Enterprise Linux Security Update for lua (ELSA-2023-0957)
<a href="#">184243</a> Debian Security Update for lua5.4 (CVE-2021-43519)
<a href="#">241222</a> Red Hat Update for lua (RHSA-2023:0957)
<a href="#">241261</a> Red Hat Update for lua (RHSA-2023:1211)
<a href="#">282349</a> Fedora Security Update for lua (FEDORA-2022-e6b2bd5b50)
<a href="#">282405</a> Fedora Security Update for lua (FEDORA-2022-473560d1a6)
<a href="#">296063</a> Oracle Solaris 11.4 Support Repository Update (SRU) 45.119.2 Missing (CPUAPR2022)
<a href="#">354467</a> Amazon Linux Security Advisory for lua : ALAS2022-2022-031
<a href="#">354526</a> Amazon Linux Security Advisory for lua : ALAS2022-2022-176
<a href="#">900450</a> Common Base Linux Mariner (CBL-Mariner) Security Update for lua (6183)
<a href="#">900940</a> Common Base Linux Mariner (CBL-Mariner) Security Update for lua (6672-1)
<a href="#">940945</a> AlmaLinux Security Update for lua (ALSA-2023:0957)
<a href="#">960895</a> Rocky Linux Security Update for lua (RLSA-2023:0957)

© [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](#)