



CVE-2020-15890

Published on: 07/21/2020 12:00:00 AM UTC

Last Modified on: 01/20/2023 08:34:00 PM UTC

CVE-2020-15890

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

Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

LuaJit through 2.1.0-beta3 has an out-of-bounds read because `__gc` handler frame traversal is mishandled.

CVE-2020-15890 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

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	NONE	NONE	HIGH

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
[SECURITY] [DLA 2296-1] luajit security update	Third Party Advisory lists.debian.org text/html	@ MLIST [debian-lts-announce] 20200728 [SECURITY] [DLA 2296-1] luajit security update
Segmentation fault in lj_err_run · Issue #601 ·	Exploit	MISC github.com/LuaJIT/LuaJIT/issues/601

LuaJIT/LuaJIT · GitHub

Third Party Advisory

github.com

text/html

USN-4501-1: LuaJIT vulnerability | Ubuntu security notices | Ubuntu

usn.ubuntu.com

text/html

 UBUNTU USN-4501-1

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

501429 Alpine Linux Security Update for luajit

Exploit/POC from Github

LuaJit through 2.1.0-beta3 has an out-of-bounds read because __gc handler frame traversal is mishandled. CVE project by

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Luajit	Luajit	2.1.0	beta1	All	All
Application	Luajit	Luajit	2.1.0	beta2	All	All
Application	Luajit	Luajit	2.1.0	beta3	All	All
Application	Luajit	Luajit	2.1.0	beta1	All	All
Application	Luajit	Luajit	2.1.0	beta2	All	All
Application	Luajit	Luajit	2.1.0	beta3	All	All
Application	Luajit	Luajit	All	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:esm:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:

cpe:2.3:a:luajit:luajit:2.1.0:beta1:*:*:*:*:*:

cpe:2.3:a:luajit:luajit:2.1.0:beta2:*:*:*:*:*:

cpe:2.3:a:luajit:luajit:2.1.0:beta3:*:*:*:*:*:

cpe:2.3:a:luajit:luajit:2.1.0:beta1:~::~::~:
cpe:2.3:a:luajit:luajit:2.1.0:beta2:~::~::~:
cpe:2.3:a:luajit:luajit:2.1.0:beta3:~::~::~:
cpe:2.3:a:luajit:luajit:~::~::~:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© [CVE.report](#) 2023   |

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](#)