CVE-2022-28805

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-28805
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-08 06:15:00 UTC
Updated	2023-11-07 03:45:00 UTC
Description	singlevar in lparser.c in Lua from (including) 5.4.0 up to (excluding) 5.4.4 lacks a certain luaK_exp2anyregup call, leading to

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Application	Lua	Lua	All	All	All	All
Application	Lua	Lua	All	All	All	All

References

Reference	Source	Link	Tags
Bug: Lua can generate wrong code when _ENV is <const> · lua/lua@1f3c6f4 · GitHub	MISC	github.com	
[SECURITY] Fedora 36 Update: lua-5.4.4-3.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
heap-buffer-overflow in luaH_getshortstr	MISC	lua-users.org	
Re: heap-buffer-overflow in luaH_getshortstr	MISC	lua-users.org	
[SECURITY] Fedora 36 Update: lua-5.4.4-3.fc36 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
Lua: Multiple Vulnerabilities (GLSA 202305-23) — Gentoo security	GENTOO	security.gentoo.org	
[SECURITY] Fedora 35 Update: lua-5.4.4-3.fc35 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 35 Update: lua-5.4.4-3.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
Re: heap-buffer-overflow in luaH_getshortstr	MISC	lua-users.org	
CVE Program record	CVE.ORG	www.cve.org	canonical

NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 160612 Oracle Enterprise Linux Security Update for lua (ELSA-2023-2582)
- 183336 Debian Security Update for lua5.4 (CVE-2022-28805)
- 241458 Red Hat Update for lua (RHSA-2023:2582)
- 282971 Fedora Security Update for lua (FEDORA-2022-b9ed35a7ad)
- 283013 Fedora Security Update for lua (FEDORA-2022-5b5889f43a)
- 296099 Oracle Solaris 11.4 Support Repository Update (SRU) 57.144.3 Missing (CPUAPR2023)
- 354423 Amazon Linux Security Advisory for lua : ALAS2022-2022-146
- 354526 Amazon Linux Security Advisory for lua : ALAS2022-2022-176
- 501752 Alpine Linux Security Update for lua5.4
- 502224 Alpine Linux Security Update for lua5.4
- 504126 Alpine Linux Security Update for lua5.4
- 710717 Gentoo Linux Lua Multiple Vulnerabilities (GLSA 202305-23)
- 900787 Common Base Linux Mariner (CBL-Mariner) Security Update for lua (9330)
- 901346 Common Base Linux Mariner (CBL-Mariner) Security Update for lua (9330-1)
- 901466 Common Base Linux Mariner (CBL-Mariner) Security Update for lua (9333)
- 902123 Common Base Linux Mariner (CBL-Mariner) Security Update for lua (9333-1)
- 904970 Common Base Linux Mariner (CBL-Mariner) Security Update for nmap (12393)
- 905026 Common Base Linux Mariner (CBL-Mariner) Security Update for nmap (12596)
- 905067 Common Base Linux Mariner (CBL-Mariner) Security Update for memcached (12565)
- 905135 Common Base Linux Mariner (CBL-Mariner) Security Update for ntopng (12600)
- 941020 AlmaLinux Security Update for lua (ALSA-2023:2582)

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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