



CVE-2020-12872

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

Summary

CVE	CVE-2020-12872
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-05-15 19:15:00 UTC
Updated	2023-11-07 03:15:00 UTC
Description	yaws_config.erl in Yaws through 2.0.2 and/or 2.0.7 loads obsolete TLS ciphers, as demonstrated by ones that allow Sweet32

Risk And Classification

Problem Types: CWE-326

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
Releases · erlyaws/yaws · GitHub	MISC	github.com	Release Notes
CVE 2020-12872. PoC of CVE 2020-12872 First of all... by CharlieLabs101 Medium		medium.com	
Sweet32: Birthday attacks on 64-bit block ciphers in TLS and OpenVPN	MISC	sweet32.info	Third Party Ad
CVE 2020-12872 - CharlieLabs101 - Medium	MISC	medium.com	Exploit, Third I
CVE-2020-12872 · Issue #402 · erlyaws/yaws · GitHub	MISC	github.com	
yaws/yaws_config.erl at c0fd79f17d52628fcec527da7fa3e788c283c445 · erlyaws/yaws · GitHub	MISC	github.com	Exploit, Third I
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[180658](#) Debian Security Update for erlang (CVE-2020-12872)

© [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](#)