



# CVE-2022-24706

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

## Summary

<b>CVE</b>	CVE-2022-24706
<b>State</b>	PUBLIC
<b>Assigner</b>	security@apache.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-04-26 10:15:00 UTC
<b>Updated</b>	2023-11-07 03:44:00 UTC
<b>Description</b>	In Apache CouchDB prior to 3.2.2, an attacker can access an improperly secured default installation without authenticating

## Risk And Classification

**EPSS:** 0.943920000 probability, percentile 0.999730000 (date 2026-04-01)

**CISA KEV:** Listed on 2022-08-25; due 2022-09-15; ransomware use Unknown

**Problem Types:** CWE-1188

## CISA Known Exploited Vulnerability

<b>Vendor</b>	Apache
<b>Product</b>	CouchDB
<b>Name</b>	Apache CouchDB Insecure Default Initialization of Resource Vulnerability
<b>Required Action</b>	Apply updates per vendor instructions.
<b>Notes</b>	<a href="https://lists.apache.org/thread/w24wo0h8n1ctfps65txvk0oc5hdcnv00">https://lists.apache.org/thread/w24wo0h8n1ctfps65txvk0oc5hdcnv00</a> ; <a href="https://nvd.nist.gov/vuln/detail/CVE-2022-24706">https://nvd.nist.gov/vuln/detail/CVE-2022-24706</a>

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Apache</a>	<a href="#">Couchdb</a>	All	All	All	All

## References

Reference	Source	Link
Apache CouchDB Erlang Remote Code Execution ≈ Packet Storm	MISC	<a href="#">packetstormsecurity.com</a>
2.2. Cluster Set Up — Apache CouchDB® 3.2 Documentation	MISC	<a href="#">docs.couchdb.org</a>
oss-security - Re: CVE-2022-24706: Apache CouchDB: Remote Code Execution Vulnerability in Packaging	MLIST	<a href="#">www.openwall.com</a>
oss-security: CVE-2022-24706: Apache CouchDB: Remote Code Execution Vulnerability in Packaging	MLIST	<a href="#">www.openwall.com</a>

oss-security - CVE-2022-24706: Apache CouchDB: Remote Code Execution Vulnerability in Packaging	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>
Apache CouchDB 3.2.1 Remote Code Execution ≈ Packet Storm	MISC	<a href="http://packetstormsecurity.com">packetstormsecurity.com</a>
<a href="https://lists.apache.org/thread/w24wo0h8nlctfps65txvk0oc5hdcnv00">lists.apache.org/thread/w24wo0h8nlctfps65txvk0oc5hdcnv00</a>	MISC	<a href="https://lists.apache.org">lists.apache.org</a>
CouchDB, Erlang and cookies — RCE on default settings   by Konstantin Burov   Medium		<a href="https://medium.com">medium.com</a>
oss-security - Re: CVE-2022-24706: Apache CouchDB: Remote Code Execution Vulnerability in Packaging	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>
oss-security - Re: CVE-2022-24706: Apache CouchDB: Remote Code Execution Vulnerability in Packaging	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>
CouchDB, Erlang and cookies — RCE on default settings   by Konstantin Burov   Medium	MISC	<a href="https://medium.com">medium.com</a>
oss-security - Re: CVE-2022-24706: Apache CouchDB: Remote Code Execution Vulnerability in Packaging	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>
CISA Known Exploited Vulnerabilities catalog	CISA	<a href="http://www.cisa.gov">www.cisa.gov</a>

### Vendor Comments And Credit

#### Discovery Credit

**LEGACY:** The Apache CouchDB Team would like to thank Alex Vandiver <[alexmv@zulip.com](mailto:alexmv@zulip.com)> for the report of this issue.

### Legacy QID Mappings

[730467](#) Apache CouchDB Remote Privilege Escalation Vulnerability

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)