



# CVE-2022-24884

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

## Summary

<b>CVE</b>	CVE-2022-24884
<b>State</b>	PUBLIC
<b>Assigner</b>	security-advisories@github.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-05-06 00:15:00 UTC
<b>Updated</b>	2023-11-07 03:44:00 UTC
<b>Description</b>	ecdsautils is a tiny collection of programs used for ECDSA (keygen, sign, verify). `ecdsa_verify_[prepare_]legacy()` does not

## Risk And Classification

**Problem Types:** CWE-347

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	11.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">Ecdsautils Project</a>	<a href="#">Ecdsautils</a>	All	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	34	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	35	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	36	All	All	All

## References

Reference	Source	Link	Ta
Debian -- Security Information -- DSA-5132-1 ecdsautils	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	
Merge pull request from GHSA-qhcg-9ffp-78pw · freifunk-gluon/ecdsautils@39b6d0a · GitHub	MISC	<a href="https://github.com">github.com</a>	
[SECURITY] Fedora 34 Update: ecdsautils-0.4.1-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 35 Update: ecdsautils-0.4.1-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 36 Update: ecdsautils-0.4.1-1.fc36 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
Improper Verification of ECDSA Signatures · Advisory · freifunk-gluon/ecdsautils · GitHub	CONFIRM	<a href="https://github.com">github.com</a>	
[SECURITY] Fedora 35 Update: ecdsautils-0.4.1-1.fc35 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	

[SECURITY] [DLA 2997-1] ecdsautils security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	
[SECURITY] Fedora 36 Update: ecdsautils-0.4.1-1.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 34 Update: ecdsautils-0.4.1-1.fc34 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
verify: fix signature verification (CVE-2022-24884) · freifunk-gluon/ecdsautils@1d4b091 · GitHub	MISC	<a href="https://github.com">github.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	ca
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	ca

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

<a href="#">179270</a> Debian Security Update for ecdsautils (DLA 2997-1)
<a href="#">179272</a> Debian Security Update for ecdsautils (DSA 5132-1)
<a href="#">183100</a> Debian Security Update for ecdsautils (CVE-2022-24884)
<a href="#">199595</a> Ubuntu Security Notification for ECDSA Util Vulnerability (USN-6239-1)
<a href="#">282691</a> Fedora Security Update for ecdsautils (FEDORA-2022-7704d5e885)
<a href="#">282692</a> Fedora Security Update for ecdsautils (FEDORA-2022-bf58612696)
<a href="#">282705</a> Fedora Security Update for ecdsautils (FEDORA-2022-111177a5ac)

© 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](https://status.cve.report)