CVE-2022-24884

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-24884
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-06 00:15:00 UTC
Updated	2023-11-07 03:44:00 UTC
Description	ecdsautils is a tiny collection of programs used for ECDSA (keygen, sign, verify). `ecdsa_verify_[prepare_]legacy()` does nc

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Ecdsautils Project	Ecdsautils	All	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All

References

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

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

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

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