



CVE-2023-40303

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2023-40303
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-14 05:15:00 UTC
Updated	2024-01-02 01:15:00 UTC
Description	GNU inetutils through 2.4 may allow privilege escalation because of unchecked return values of set*id() family functions in f

Risk And Classification

Problem Types: CWE-252

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Inetutils	All	All	All	All

References

Reference

[oss-security] 20231230 Re: inetutils ftpd, rcp, rlogin, rsh, rshd, uucpd: Avoid potential privilege escalations by checking set*id() return values

[SECURITY] [DLA 3611-1] inetutils security update

Index of /gnu/inetutils

inetutils.git - GNU Inetutils

setuid/setgid return values not checked in rlogin, rsh, rshd and uucpd

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[199675](#) Ubuntu Security Notification for Inetutils Vulnerabilities (USN-6304-1)

[6000079](#) Debian Security Update for inetutils (DLA 3611-1)

© [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](#)