



net-tools Stack-based Buffer Overflow vulnerability

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

Summary

CVE	CVE-2025-46836
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-05-14 23:15:48 UTC
Updated	2026-05-12 13:17:19 UTC
Description	net-tools is a collection of programs that form the base set of the NET-3 networking distribution for the Linux operating system.

Risk And Classification

Primary CVSS: v3.1 6.6 MEDIUM from security-advisories@github.com

CVSS: 3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H

EPSS: 0.001370000 probability, percentile 0.331810000 (date 2026-05-12)

Problem Types: CWE-20 | CWE-121 | CWE-20 CWE-20: Improper Input Validation | CWE-121 CWE-121: Stack-based Buffer Overflow

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	6.6	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H
3.1	CNA	DECLARED	6.6	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

ntegrity

Low

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Ecki	Net-tools	affected <= 2.10	Not specified
ADP	Siemens	RUGGEDCOM ROX MX5000	affected V2.17.1 custom	Not specified
ADP	Siemens	RUGGEDCOM ROX MX5000RE	affected V2.17.1 custom	Not specified
ADP	Siemens	RUGGEDCOM ROX RX1400	affected V2.17.1 custom	Not specified
ADP	Siemens	RUGGEDCOM ROX RX1500	affected V2.17.1 custom	Not specified
ADP	Siemens	RUGGEDCOM ROX RX1501	affected V2.17.1 custom	Not specified
ADP	Siemens	RUGGEDCOM ROX RX1510	affected V2.17.1 custom	Not specified
ADP	Siemens	RUGGEDCOM ROX RX1511	affected V2.17.1 custom	Not specified
ADP	Siemens	RUGGEDCOM ROX RX1512	affected V2.17.1 custom	Not specified
ADP	Siemens	RUGGEDCOM ROX RX1524	affected V2.17.1 custom	Not specified
ADP	Siemens	RUGGEDCOM ROX RX1536	affected V2.17.1 custom	Not specified
ADP	Siemens	RUGGEDCOM ROX RX5000	affected V2.17.1 custom	Not specified
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom	Not specified
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom	Not specified
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.5 * custom	Not specified
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.5 * custom	Not specified
ADP	Siemens	SIPLUS S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom	Not specified

References

Reference	Source	Link
github.com/ecki/net-tools/commit/7a8f42fb20013a1493d8cae1c43436f85e656f2d	security-advisories@github.com	github.com
lists.debian.org/debian-lts-announce/2025/05/msg00053.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.c
cert-portal.siemens.com/productcert/html/ssa-082556.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.si
cert-portal.siemens.com/productcert/html/ssa-577017.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.si
github.com/ecki/net-tools/security/advisories/GHSA-pfwf-h6m3-63wf	security-advisories@github.com	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#)