



CVE-2011-2502

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

Summary

CVE	CVE-2011-2502
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-07-26 19:55:00 UTC
Updated	2026-04-29 01:13:23 UTC
Description	runtime/staprun/staprun_funcs.c in the systemtap runtime tool (staprun) in SystemTap before 1.6 does not properly validate

Risk And Classification

Primary CVSS: v2.0 4.4 from nvd@nist.gov

AV:L/AC:M/Au:N/C:P/I:P/A:P

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:L/AC:M/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Systemtap	Systemtap	0.2.2	All	All	All

Application	Systemtap	Systemtap	0.3	All	All	All
Application	Systemtap	Systemtap	0.4	All	All	All
Application	Systemtap	Systemtap	0.5	All	All	All
Application	Systemtap	Systemtap	0.5.10	All	All	All
Application	Systemtap	Systemtap	0.5.12	All	All	All
Application	Systemtap	Systemtap	0.5.13	All	All	All
Application	Systemtap	Systemtap	0.5.14	All	All	All
Application	Systemtap	Systemtap	0.5.3	All	All	All
Application	Systemtap	Systemtap	0.5.4	All	All	All
Application	Systemtap	Systemtap	0.5.5	All	All	All
Application	Systemtap	Systemtap	0.5.7	All	All	All
Application	Systemtap	Systemtap	0.5.8	All	All	All
Application	Systemtap	Systemtap	0.5.9	All	All	All
Application	Systemtap	Systemtap	0.6	All	All	All
Application	Systemtap	Systemtap	0.6.2	All	All	All
Application	Systemtap	Systemtap	0.7	All	All	All
Application	Systemtap	Systemtap	0.7.2	All	All	All
Application	Systemtap	Systemtap	0.8	All	All	All
Application	Systemtap	Systemtap	0.9	All	All	All
Application	Systemtap	Systemtap	0.9.5	All	All	All
Application	Systemtap	Systemtap	0.9.7	All	All	All
Application	Systemtap	Systemtap	0.9.8	All	All	All
Application	Systemtap	Systemtap	0.9.9	All	All	All
Application	Systemtap	Systemtap	1.0	All	All	All
Application	Systemtap	Systemtap	1.1	All	All	All
Application	Systemtap	Systemtap	1.2	All	All	All
Application	Systemtap	Systemtap	1.3	All	All	All
Application	Systemtap	Systemtap	1.4	All	All	All
Application	Systemtap	Systemtap	All	All	All	All

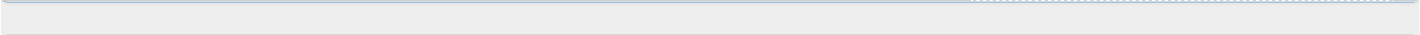
Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
SystemTap "leakage" Privilege Escalation Security Issue	Secunia.com

Systemtap: staprun: Privilege Escalation Security Issues - Secunia.com	af854a3a-2127-422b-91ae-364d
www.sourceware.org Git - systemtap.git/blob - NEWS	af854a3a-2127-422b-91ae-364d
Bug 716476 – CVE-2011-2502 systemtap: insufficient security check when loading uprobes kernel module	af854a3a-2127-422b-91ae-364d
www.sourceware.org Git - systemtap.git/commitdiff	af854a3a-2127-422b-91ae-364d
www.sourceware.org Git - systemtap.git/blob - NEWS	MITRE
www.sourceware.org Git - systemtap.git/commitdiff	MITRE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD



No vendor comments have been submitted for this CVE.

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