CVE-2010-0411

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2010-0411
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-02-08 20:30:01 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Multiple integer signedness errors in the (1) __get_argv and (2) __get_compat_argv functions in tapset/aux_syscalls.stp in

Risk And Classification

Primary CVSS: v2.0 4.9 from nvd@nist.gov

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

Problem Types: CWE-189 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Systemtap	Systemtap	1.1	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
[security-announce] SUSE Security Summary Report: SUSE-SR:2010:010	af854a3a-2127-422b-91ae-364
11234 – __get_argv can overflow its return buffer	af854a3a-2127-422b-91ae-364
Red Hat update for systemtap - Secunia.com	af854a3a-2127-422b-91ae-364
SystemTap Buffer Overflow Vulnerabilities - Advisories - Community	af854a3a-2127-422b-91ae-364
Support	af854a3a-2127-422b-91ae-364
SUSE update for Multiple Packages - Advisories - Community	af854a3a-2127-422b-91ae-364
[SECURITY] Fedora 12 Update: systemtap-1.1-2.fc12	af854a3a-2127-422b-91ae-364
Fedora update for systemtap - Secunia.com	af854a3a-2127-422b-91ae-364
SystemTap Buffer Overflow in __get_argv() May Let Local Users Gain Elevated Privileges - SecurityTracker	af854a3a-2127-422b-91ae-364
Support	af854a3a-2127-422b-91ae-364
sourceware.org Git - systemtap.git/commit	af854a3a-2127-422b-91ae-364
[SECURITY] Fedora 11 Update: systemtap-1.1-2.fc11	af854a3a-2127-422b-91ae-364
559719 – (CVE-2010-0411) CVE-2010-0411 systemtap: Crash with systemtap script using __get_argv()	af854a3a-2127-422b-91ae-364
SystemTap '__get_argv()' and '__get_compat_argv()' Local Memory Corruption Vulnerabilities	af854a3a-2127-422b-91ae-364
Red Hat update for systemtap - Secunia.com	af854a3a-2127-422b-91ae-364
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364
'[oss-security] systemtap DoS issue (CVE-2010-0411)' - MARC	af854a3a-2127-422b-91ae-364
Repository / Oval Repository	af854a3a-2127-422b-91ae-364
sourceware.org Git - systemtap.git/commit	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.

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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**