CVE-2010-0412

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

Summary

CVE	CVE-2010-0412
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-02-25 00:30:00 UTC
Updated	2026-04-29 01:13:23 UTC
Description	stap-server in SystemTap 1.1 does not properly restrict the value of the -B (aka BUILD) option, which allows attackers to ha

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

Problem Types: NVD-CWE-noinfo | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/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	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] Fedora 12 Update: systemtap-1.1-2.fc12	af854a3a-2127-422b-91ae
rpms/systemtap/devel systemtap-1.1-tighten-server-params.patch, NONE, 1.1 systemtap.spec, 1.59, 1.60	af854a3a-2127-422b-91ae
[SECURITY] Fedora 11 Update: systemtap-1.1-2.fc11	af854a3a-2127-422b-91ae
SystemTap Remote Arbitrary Command Execution Vulnerability	af854a3a-2127-422b-91ae
IBM X-Force Exchange	af854a3a-2127-422b-91ae
CVE-2010-0412 - Red Hat Customer Portal	MITRE
550172 – (CVE-2009-4273, CVE-2010-0412) CVE-2009-4273 systemtap: remote code execution via stap-server	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.