CVE-2005-1751

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

Summary

CVE	CVE-2005-1751
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-05-25 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Race condition in shtool 2.0.1 and earlier allows local users to create or modify arbitrary files via a symlink attack on the .sh

Risk And Classification

Primary CVSS: v2.0 3.7 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

High

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Shtool	Shtool	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
Repository / Oval Repository	af854a3a-2127-422b-91ae-364da26611
Secunia - Advisories - Gentoo update for shtool/ocaml-mysql	af854a3a-2127-422b-91ae-364da26611
ZATAZ » Page non trouvée	af854a3a-2127-422b-91ae-364da26611
Gentoo Bug 93782 - dev-util/shtool <= 2.0.1 insecure temporary file creation (CAN-2005-175{1-9})	af854a3a-2127-422b-91ae-364da26611
Gentoo Linux Documentation -- GNU shtool, ocaml-mysql: Insecure temporary file creation	af854a3a-2127-422b-91ae-364da26611
SecurityTracker.com Archives - shtool Temporary File May Let Local users gain Elevated Privileges	af854a3a-2127-422b-91ae-364da26611
'[OpenPKG-SA-2005.011] OpenPKG Security Advisory (shtool)' - MARC	af854a3a-2127-422b-91ae-364da26611
Repository / Oval Repository	af854a3a-2127-422b-91ae-364da26611
rhn.redhat.com | Red Hat Support	af854a3a-2127-422b-91ae-364da26611
GNU SHTool Insecure Temporary File Deletion Vulnerability	af854a3a-2127-422b-91ae-364da26611
GNU shtool Insecure Temporary File Creation - Secunia.com	af854a3a-2127-422b-91ae-364da26611
Debian -- Security Information -- DSA-789-1 php4	af854a3a-2127-422b-91ae-364da26611
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2006-09-19	Mark J Cox	Red Hat is aware of this issue and is tracking it via the following bug: https://bugzilla.redhat.com/

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