



CVE-2007-6350

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

Summary

CVE	CVE-2007-6350
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-12-14 20:46:00 UTC
Updated	2011-08-08 04:00:00 UTC
Description	scponly 4.6 and earlier allows remote authenticated users to bypass intended restrictions and execute code by invoking dar

Risk And Classification

Problem Types: CWE-264 | NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Scponly	Scponly	4.2	All	All	All
Application	Scponly	Scponly	4.3	All	All	All
Application	Scponly	Scponly	4.4	All	All	All
Application	Scponly	Scponly	4.5	All	All	All
Application	Scponly	Scponly	4.2	All	All	All
Application	Scponly	Scponly	4.3	All	All	All
Application	Scponly	Scponly	4.4	All	All	All
Application	Scponly	Scponly	4.5	All	All	All
Application	Scponly	Scponly	All	All	All	All

References

Reference	Source
#437148 - "svn", "svnserve", "unison", "rsync" passthrough is unsafe - Debian Bug report logs	CONFIRM
Fedora update for scponly - Secunia.com	SECUNIA
Gentoo Bug 201726 - net-misc/scponly - svn, svnserve, unison and rsync passthrough is unsafe by design (CVE-2007-6350)	CONFIRM
scponly Local Arbitrary Command Execution Weakness	BID
Webmail - OVH	VUPEN

[SECURITY] Fedora 8 Update: scponly-4.6-10.fc8	FEDORA
scponly Command Passthrough Security Bypass - Advisories - Secunia	SECUNIA
CVS Info for project scponly	CONFIRM
Debian update for scponly - Advisories - Secunia	SECUNIA
[SECURITY] Fedora 7 Update: scponly-4.6-10.fc7	FEDORA
44137	OSVDB
Debian -- Security Information -- DSA-1473-1 scponly	DEBIAN
Scponly May Let Remote Authenticated Users Execute Arbitrary Commands - SecurityTracker	SECTrack
Gentoo update for scponly - Advisories - Secunia	SECUNIA
Gentoo Linux Documentation -- scponly: Multiple vulnerabilities	GENTOO
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.

© [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](#)