CVE-2015-0853

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

Summary

CVE	CVE-2015-0853
State	PUBLIC
Assigner	security@debian.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-09-06 21:29:00 UTC
Updated	2021-09-09 17:43:00 UTC
Description	svn-workbench 1.6.2 and earlier on a system with xeyes installed allows local users to execute arbitrary commands by usin

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pysvn	Svn-workbench	All	All	All	All
Application	Pysvn Project	Svn-workbench	All	All	All	All

References

Reference	Source	Link	Tags
pysvn.tigris.org/issues/show_bug.cgi	MISC	pysvn.tigris.org	Exploit,
oss-security - CVE-2015-0853: insecure use of os.system() in svn-workbench	MLIST	www.openwall.com	Exploit,
Bug #1495268 “insecure use of os.system()” : Bugs : svn-workbench package : Ubuntu	MISC	bugs.launchpad.net	Issue T
#798863 - CVE-2015-0853: insecure use of os.system() - Debian Bug report logs	MISC	bugs.debian.org	Exploit,
1262928 – (CVE-2015-0853) CVE-2015-0853 pysvn: Insecure use of os.system() in Workbench	CONFIRM	bugzilla.redhat.com	Issue T
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report