



CVE-2009-0316

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

Summary

CVE	CVE-2009-0316
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-01-28 11:30:00 UTC
Updated	2017-08-08 01:33:00 UTC
Description	Untrusted search path vulnerability in src/if_python.c in the Python interface in Vim before 7.2.045 allows local users to exe

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vim	Vim	1.0	All	All	All
Application	Vim	Vim	1.22	All	All	All
Application	Vim	Vim	3.0	All	All	All
Application	Vim	Vim	4.0	All	All	All
Application	Vim	Vim	5.0	All	All	All
Application	Vim	Vim	5.1	All	All	All
Application	Vim	Vim	5.2	All	All	All
Application	Vim	Vim	5.3	All	All	All
Application	Vim	Vim	5.4	All	All	All
Application	Vim	Vim	5.5	All	All	All
Application	Vim	Vim	5.6	All	All	All
Application	Vim	Vim	5.7	All	All	All
Application	Vim	Vim	5.8	All	All	All
Application	Vim	Vim	6.0	All	All	All
Application	Vim	Vim	6.1	All	All	All
Application	Vim	Vim	6.2	All	All	All
Application	Vim	Vim	6.3	All	All	All

Application	Vim	Vim	6.4	All	All	All
Application	Vim	Vim	7.0	All	All	All
Application	Vim	Vim	7.1	All	All	All
Application	Vim	Vim	1.0	All	All	All
Application	Vim	Vim	1.22	All	All	All
Application	Vim	Vim	3.0	All	All	All
Application	Vim	Vim	4.0	All	All	All
Application	Vim	Vim	5.0	All	All	All
Application	Vim	Vim	5.1	All	All	All
Application	Vim	Vim	5.2	All	All	All
Application	Vim	Vim	5.3	All	All	All
Application	Vim	Vim	5.4	All	All	All
Application	Vim	Vim	5.5	All	All	All
Application	Vim	Vim	5.6	All	All	All
Application	Vim	Vim	5.7	All	All	All
Application	Vim	Vim	5.8	All	All	All
Application	Vim	Vim	6.0	All	All	All
Application	Vim	Vim	6.1	All	All	All
Application	Vim	Vim	6.2	All	All	All
Application	Vim	Vim	6.3	All	All	All
Application	Vim	Vim	6.4	All	All	All
Application	Vim	Vim	7.0	All	All	All
Application	Vim	Vim	7.1	All	All	All
Application	Vim	Vim	All	All	All	All

References

Reference

#493937 - bicyclerepair: bike.vim imports untrusted python files from cwd - Debian Bug report logs

Support / Security / Advisories // MDVSA-2009:047 | Mandriva

IBM X-Force Exchange

oss-security - CVE request -- Python < 2.6 PySys_SetArgv issues (epiphany, csound, dia, eog, gedit, xchat, vim, nautilus-python, Gnumeric)

Bug 481565 – CVE-2009-0316 vim: untrusted python modules search path

APPLE-SA-2010-03-29-1 Security Update 2010-002 / Mac OS X v10.6.3

Old Nabble - debian-bugs-rc - Bug#484305: bicyclerepair: bike.vim imports untrusted python files from cwd

#484305 - bicyclerepair: bike.vim imports untrusted python files from cwd - Debian Bug report logs

VIM: CVE-2009-0316: vim: untrusted python modules search path

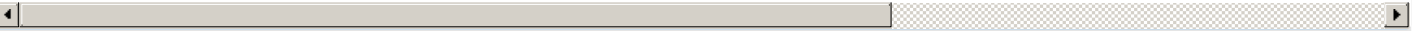
Vim 'PySys_SetArgv' Remote Command Execution Vulnerability

About the security content of Security Update 2010-002 / Mac OS X v10.6.3

svn.pardus.org.tr/pardus/2008/applications/editors/vim/files/official/7.2.045

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

753066 SUSE Enterprise Linux Security Update for vim (SUSE-SU-2022:4619-1)

© [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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)