



CVE-2006-4980

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2006-4980
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-10-10 04:06:00 UTC
Updated	2023-08-02 18:04:00 UTC
Description	Buffer overflow in the repr function in Python 2.3 through 2.6 before 20060822 allows context-dependent attackers to cause

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Python	Python	All	All	All	All
Application	Python Software Foundation	Python	2.3	All	All	All
Application	Python Software Foundation	Python	2.3.1	All	All	All
Application	Python Software Foundation	Python	2.3.2	All	All	All
Application	Python Software Foundation	Python	2.3.3	All	All	All
Application	Python Software Foundation	Python	2.3.4	All	All	All
Application	Python Software Foundation	Python	2.3.5	All	All	All
Application	Python Software Foundation	Python	2.4	All	All	All
Application	Python Software Foundation	Python	2.4.2	All	All	All
Application	Python Software Foundation	Python	2.4.3	All	All	All
Application	Python Software Foundation	Python	2.5_alpha_1	All	All	All
Application	Python Software Foundation	Python	2.5_alpha_2	All	All	All
Application	Python Software Foundation	Python	2.5_beta_1	All	All	All
Application	Python Software Foundation	Python	2.5_beta_2	All	All	All
Application	Python Software Foundation	Python	2.5_beta_3	All	All	All
Application	Python Software Foundation	Python	2.5_final	All	All	All
Application	Python Software Foundation	Python	2.5_release_candidate_1	All	All	All

Application	Python Software Foundation	Python	2.5_release_candidate_2	All	All	All
Application	Python Software Foundation	Python	2.3	All	All	All
Application	Python Software Foundation	Python	2.3.1	All	All	All
Application	Python Software Foundation	Python	2.3.2	All	All	All
Application	Python Software Foundation	Python	2.3.3	All	All	All
Application	Python Software Foundation	Python	2.3.4	All	All	All
Application	Python Software Foundation	Python	2.3.5	All	All	All
Application	Python Software Foundation	Python	2.4	All	All	All
Application	Python Software Foundation	Python	2.4.2	All	All	All
Application	Python Software Foundation	Python	2.4.3	All	All	All
Application	Python Software Foundation	Python	2.5_alpha_1	All	All	All
Application	Python Software Foundation	Python	2.5_alpha_2	All	All	All
Application	Python Software Foundation	Python	2.5_beta_1	All	All	All
Application	Python Software Foundation	Python	2.5_beta_2	All	All	All
Application	Python Software Foundation	Python	2.5_beta_3	All	All	All
Application	Python Software Foundation	Python	2.5_final	All	All	All
Application	Python Software Foundation	Python	2.5_release_candidate_1	All	All	All
Application	Python Software Foundation	Python	2.5_release_candidate_2	All	All	All

References

Reference

[Red Hat update for python - Advisories - Secunia](#)

[Repository / Oval Repository](#)

[Ubuntu update for python - Advisories - Secunia](#)

[Gentoo Linux Documentation -- Python: Buffer Overflow](#)

[208162 – CVE-2006-4980 repr unicode buffer overflow](#)

[SGI Advanced Linux Environment Multiple Updates - Advisories - Secunia](#)

Support

[usn/usn-359-1 - Ubuntu: Linux for human beings](#)

[Bug #56633 in python2.4 \(Ubuntu\): "buffer overrun in repr\(\) for unicode strings"](#)

[Download Patch ESX-9986131 for VMware ESX Server 3.0.1](#)

[VMWare ESX Server Multiple Vulnerabilities - Advisories - Secunia](#)

[Python Repr\(\) Function Remote Code Execution Vulnerability](#)

Support

[Mandriva update for python - Secunia Advisories - Vulnerability Intelligence - Secunia.com](#)

Security Tracker.com Archives - Python repr() Processing of UTF-32/UCS-4 Strings May Let Remote Users Deny Service or Execute Arbitrary

Debian update for python2.4 - Secunia Advisories - Vulnerability Intelligence - Secunia.com

#391589 - [CVE-2006-4980] buffer overrun in repr() for unicode strings - Debian Bug report logs

[#RPL-702] Buffer overflow in Python's repr function creates vulnerabilities in some python applications CVE-2006-4980 - rPath JIRA

SourceForge.net: ERROR

Security Announcement

rPath update for idle and python - Advisories - Secunia

Avaya Python "repr()" Unicode String Buffer Overflow Vulnerability - Advisories - Secunia

20061001-01-P

SUSE Update for Multiple Packages - Advisories - Secunia

Advisories - Mandriva Linux

IBM X-Force Exchange

zoehep.xent.com/~bsittler/python2.4-2.4.3_unicodeobject.c.diff

Debian update for python2.3 - Advisories - Secunia

Debian -- Security Information -- DSA-1197-1 python2.4

VMware Knowledge Base

ASA-2006-229 (RHSA-2006-0713)

Gentoo update for python - Advisories - Secunia

Webmail - OVH

Webmail - OVH

SecurityFocus

Debian -- Security Information -- DSA-1198-1 python2.3

Download Patch ESX-3069097 for VMware ESX Server 3.0.1

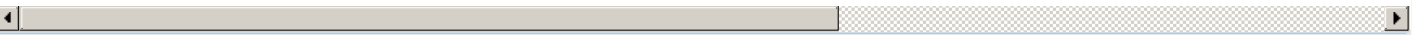
Red Hat Network Satellite Server Update for Solaris Client - Advisories - Community

SecurityFocus

Python "repr()" Unicode String Buffer Overflow Vulnerability - Advisories - Secunia

CVE Program record

NVD vulnerability detail



Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-03-14	Mark J Cox	Red Hat Enterprise Linux 5 is not vulnerable to this issue as it contains a backported patch.

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](#).

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