



CVE-2006-0847

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

Summary

CVE	CVE-2006-0847
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-02-22 02:02:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Directory traversal vulnerability in the staticfilter component in CherryPy before 2.1.1 allows remote attackers to read arbitra

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

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

EPSS: 0.006390000 probability, percentile 0.705540000 (date 2026-04-16)

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
------	--------	---------	---------	--------	---------	----------

Application	CherryPy	CherryPy	0.1	All	All	All
Application	CherryPy	CherryPy	0.10	All	All	All
Application	CherryPy	CherryPy	0.10_beta	All	All	All
Application	CherryPy	CherryPy	0.10_rc1	All	All	All
Application	CherryPy	CherryPy	0.2	All	All	All
Application	CherryPy	CherryPy	0.3	All	All	All
Application	CherryPy	CherryPy	0.4	All	All	All
Application	CherryPy	CherryPy	0.5	All	All	All
Application	CherryPy	CherryPy	0.6	All	All	All
Application	CherryPy	CherryPy	0.7	All	All	All
Application	CherryPy	CherryPy	0.8	All	All	All
Application	CherryPy	CherryPy	0.8_beta	All	All	All
Application	CherryPy	CherryPy	0.9	All	All	All
Application	CherryPy	CherryPy	0.9_beta	All	All	All
Application	CherryPy	CherryPy	0.9_gamma	All	All	All
Application	CherryPy	CherryPy	0.9_rc1	All	All	All
Application	CherryPy	CherryPy	2.0.0	All	All	All
Application	CherryPy	CherryPy	2.0.0a1	All	All	All
Application	CherryPy	CherryPy	2.1.0	All	All	All
Application	CherryPy	CherryPy	2.1.0_beta	All	All	All
Application	CherryPy	CherryPy	2.1.0_rc1	All	All	All
Application	CherryPy	CherryPy	2.1.0_rc2	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References						
Reference			Source		Link	
CherryPy StaticFilter Directory Traversal Vulnerability			af854a3a-2127-422b-91ae-364da2661108		www.securityfocus.com	
CherryPy download SourceForge.net			af854a3a-2127-422b-91ae-364da2661108		sourceforge.net	
CherryPy - Trac			af854a3a-2127-422b-91ae-364da2661108		www.cherrypy.org	
Secunia - Advisories - Gentoo update for cherrypy			af854a3a-2127-422b-91ae-364da2661108		secunia.com	
مجموعات Google			af854a3a-2127-422b-91ae-364da2661108		groups.google.co	
Gentoo Linux Documentation -- CherryPy: Directory traversal vulnerability			af854a3a-2127-422b-91ae-364da2661108		www.gentoo.org	
CherryPy "staticfilter" Directory Traversal Vulnerability - Advisories - Secunia			af854a3a-2127-422b-91ae-364da2661108		secunia.com	

IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108	exchange.xforce.
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2661108	www.vupen.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/licenses).

Free CVE JSON API cve.report/api

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