



# CVE-2005-2390

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2005-2390
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2005-07-27 04:00:00 UTC
<b>Updated</b>	2016-10-18 03:26:00 UTC
<b>Description</b>	Multiple format string vulnerabilities in ProFTPD before 1.3.0rc2 allow attackers to cause a denial of service or obtain sensi

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Proftpd Project</a>	<a href="#">Proftpd</a>	1.2.0_pre10	All	All	All
Application	<a href="#">Proftpd Project</a>	<a href="#">Proftpd</a>	1.2.0_pre9	All	All	All
Application	<a href="#">Proftpd Project</a>	<a href="#">Proftpd</a>	1.2.0_rc1	All	All	All
Application	<a href="#">Proftpd Project</a>	<a href="#">Proftpd</a>	1.2.0_rc2	All	All	All
Application	<a href="#">Proftpd Project</a>	<a href="#">Proftpd</a>	1.2.0_rc3	All	All	All
Application	<a href="#">Proftpd Project</a>	<a href="#">Proftpd</a>	1.2.1	All	All	All
Application	<a href="#">Proftpd Project</a>	<a href="#">Proftpd</a>	1.2.10	All	All	All
Application	<a href="#">Proftpd Project</a>	<a href="#">Proftpd</a>	1.2.10_rc1	All	All	All
Application	<a href="#">Proftpd Project</a>	<a href="#">Proftpd</a>	1.2.10_rc2	All	All	All
Application	<a href="#">Proftpd Project</a>	<a href="#">Proftpd</a>	1.2.10_rc3	All	All	All
Application	<a href="#">Proftpd Project</a>	<a href="#">Proftpd</a>	1.2.1_final	All	All	All
Application	<a href="#">Proftpd Project</a>	<a href="#">Proftpd</a>	1.2.2	All	All	All
Application	<a href="#">Proftpd Project</a>	<a href="#">Proftpd</a>	1.2.2_rc1	All	All	All
Application	<a href="#">Proftpd Project</a>	<a href="#">Proftpd</a>	1.2.2_rc2	All	All	All
Application	<a href="#">Proftpd Project</a>	<a href="#">Proftpd</a>	1.2.2_rc3	All	All	All
Application	<a href="#">Proftpd Project</a>	<a href="#">Proftpd</a>	1.2.3	All	All	All
Application	<a href="#">Proftpd Project</a>	<a href="#">Proftpd</a>	1.2.4	All	All	All

Application	Proftpd Project	Proftpd	1.2.5	All	All	All
Application	Proftpd Project	Proftpd	1.2.5_rc1	All	All	All
Application	Proftpd Project	Proftpd	1.2.5_rc2	All	All	All
Application	Proftpd Project	Proftpd	1.2.5_rc3	All	All	All
Application	Proftpd Project	Proftpd	1.2.6	All	All	All
Application	Proftpd Project	Proftpd	1.2.6_rc1	All	All	All
Application	Proftpd Project	Proftpd	1.2.6_rc2	All	All	All
Application	Proftpd Project	Proftpd	1.2.6_rc3	All	All	All
Application	Proftpd Project	Proftpd	1.2.7	All	All	All
Application	Proftpd Project	Proftpd	1.2.7_rc1	All	All	All
Application	Proftpd Project	Proftpd	1.2.7_rc2	All	All	All
Application	Proftpd Project	Proftpd	1.2.7_rc3	All	All	All
Application	Proftpd Project	Proftpd	1.2.8	All	All	All
Application	Proftpd Project	Proftpd	1.2.8_rc1	All	All	All
Application	Proftpd Project	Proftpd	1.2.8_rc2	All	All	All
Application	Proftpd Project	Proftpd	1.2.9	All	All	All
Application	Proftpd Project	Proftpd	1.2.9_rc1	All	All	All
Application	Proftpd Project	Proftpd	1.2.9_rc2	All	All	All
Application	Proftpd Project	Proftpd	1.2.9_rc3	All	All	All
Application	Proftpd Project	Proftpd	1.3.0_rc1	All	All	All
Application	Proftpd Project	Proftpd	1.2.0_pre10	All	All	All
Application	Proftpd Project	Proftpd	1.2.0_pre9	All	All	All
Application	Proftpd Project	Proftpd	1.2.0_rc1	All	All	All
Application	Proftpd Project	Proftpd	1.2.0_rc2	All	All	All
Application	Proftpd Project	Proftpd	1.2.0_rc3	All	All	All
Application	Proftpd Project	Proftpd	1.2.1	All	All	All
Application	Proftpd Project	Proftpd	1.2.10	All	All	All
Application	Proftpd Project	Proftpd	1.2.10_rc1	All	All	All
Application	Proftpd Project	Proftpd	1.2.10_rc2	All	All	All
Application	Proftpd Project	Proftpd	1.2.10_rc3	All	All	All
Application	Proftpd Project	Proftpd	1.2.1_final	All	All	All
Application	Proftpd Project	Proftpd	1.2.2	All	All	All
Application	Proftpd Project	Proftpd	1.2.2_rc1	All	All	All
Application	Proftpd Project	Proftpd	1.2.2_rc2	All	All	All
Application	Proftpd Project	Proftpd	1.2.2_rc3	All	All	All

Application	Proftpd Project	Proftpd	1.2.3	All	All	All
Application	Proftpd Project	Proftpd	1.2.4	All	All	All
Application	Proftpd Project	Proftpd	1.2.5	All	All	All
Application	Proftpd Project	Proftpd	1.2.5_rc1	All	All	All
Application	Proftpd Project	Proftpd	1.2.5_rc2	All	All	All
Application	Proftpd Project	Proftpd	1.2.5_rc3	All	All	All
Application	Proftpd Project	Proftpd	1.2.6	All	All	All
Application	Proftpd Project	Proftpd	1.2.6_rc1	All	All	All
Application	Proftpd Project	Proftpd	1.2.6_rc2	All	All	All
Application	Proftpd Project	Proftpd	1.2.6_rc3	All	All	All
Application	Proftpd Project	Proftpd	1.2.7	All	All	All
Application	Proftpd Project	Proftpd	1.2.7_rc1	All	All	All
Application	Proftpd Project	Proftpd	1.2.7_rc2	All	All	All
Application	Proftpd Project	Proftpd	1.2.7_rc3	All	All	All
Application	Proftpd Project	Proftpd	1.2.8	All	All	All
Application	Proftpd Project	Proftpd	1.2.8_rc1	All	All	All
Application	Proftpd Project	Proftpd	1.2.8_rc2	All	All	All
Application	Proftpd Project	Proftpd	1.2.9	All	All	All
Application	Proftpd Project	Proftpd	1.2.9_rc1	All	All	All
Application	Proftpd Project	Proftpd	1.2.9_rc2	All	All	All
Application	Proftpd Project	Proftpd	1.2.9_rc3	All	All	All
Application	Proftpd Project	Proftpd	1.3.0_rc1	All	All	All

## References

Reference	Source	Link	Tags
ProFTPD Shutdown Message Format String Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	
404 Not Found	CONFIRM	<a href="http://www.proftpd.org">www.proftpd.org</a>	
Secunia - Advisories - ProFTPD Two Format String Vulnerabilities	SECUNIA	<a href="http://secunia.com">secunia.com</a>	Vendor Advisory
'[OpenPKG-SA-2005.020] OpenPKG Security Advisory (proftpd)' - MARC	OPENPKG	<a href="http://marc.info">marc.info</a>	
ProFTPD SQLShowInfo SQL Output Format String Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	
Debian -- Security Information -- DSA-795-2 proftpd	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

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](#).

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