



# CVE-2006-6563

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

## Summary

<b>CVE</b>	CVE-2006-6563
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2006-12-15 11:28:00 UTC
<b>Updated</b>	2018-10-17 21:49:00 UTC
<b>Description</b>	Stack-based buffer overflow in the pr_ctrls_rcv_request function in ctrl.c in the mod_ctrls module in ProFTPD before 1.3.0a.

## 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>	1.3.0	All	All	All
Application	<a href="#">Proftpd Project</a>	<a href="#">Proftpd</a>	1.3.0a	All	All	All
Application	<a href="#">Proftpd Project</a>	<a href="#">Proftpd</a>	1.3.0	All	All	All
Application	<a href="#">Proftpd Project</a>	<a href="#">Proftpd</a>	1.3.0a	All	All	All

## References

Reference	Source	Link	Tags
ProFTPD 1.3.0/1.3.0a (mod_ctrls support) Local Buffer Overflow Exploit	EXPLOIT-DB	<a href="http://www.exploit-db.com">www.exploit-db.com</a>	
OpenPKG Corporation: Security: Security Advisories	OPENPKG	<a href="http://www.openpkg.com">www.openpkg.com</a>	
ProFTPD "mod_ctrls" Privilege Escalation Vulnerability - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>	Exploit, Pat
Mandriva update for proftpd - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>	
Gentoo Linux Documentation -- ProFTPD: Local privilege escalation	GENTOO	<a href="http://security.gentoo.org">security.gentoo.org</a>	
SecurityFocus	BUGTRAQ	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	
Core Security   CoreLabs	MISC	<a href="http://www.coresecurity.com">www.coresecurity.com</a>	Exploit, Pat
Webmail - OVH	VUPEN	<a href="http://www.vupen.com">www.vupen.com</a>	
404 Not Found	CONFIRM	<a href="http://www.proftpd.org">www.proftpd.org</a>	
Gentoo update for proftpd - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>	

SecurityFocus	BUGTRAQ	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	
Advisories - Mandriva Linux	MANDRIVA	<a href="http://www.mandriva.com">www.mandriva.com</a>	
Trustix update for proftpd - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>	
ProFTPD Controls Module Local Buffer Overflow Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	Exploit, Pat
SecurityFocus	BUGTRAQ	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	
IBM X-Force Exchange	XF	<a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>	
2006-0074	TRUSTIX	<a href="http://www.trustix.org">www.trustix.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, c

No vendor comments have been submitted for this CVE.

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

© [CVE.report](http://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](http://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://MITRE's CVE web site). This site includes MITRE data granted under the following [license](http://license).

**CVE.report and Source URL Uptime Status** [status.cve.report](http://status.cve.report)