



# CVE-2006-5815

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

## Summary

<b>CVE</b>	CVE-2006-5815
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2006-11-08 23:07:00 UTC
<b>Updated</b>	2018-10-17 21:45:00 UTC
<b>Description</b>	Stack-based buffer overflow in the sreplace function in ProFTPD 1.3.0 and earlier allows remote attackers, probably authen

## Risk And Classification

### Problem Types: CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Proftpd Project</a>	<a href="#">Proftpd</a>	All	All	All	All

## References

Reference	Source	Link
Gentoo Linux Documentation -- ProFTPD: Remote execution of arbitrary code	GENTOO	<a href="http://www.gentoo.org">www.gentoo.org</a>
2006-0066	TRUSTIX	<a href="http://www.trustix.com">www.trustix.com</a>
Mandriva update for proftpd - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>
ProFTPD "CommandBufferSize" Denial of Service Vulnerability - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>
Debian update for proftpd - Secunia.com	SECUNIA	<a href="http://secunia.com">secunia.com</a>
Debian -- Security Information -- DSA-1222-2 proftpd	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>
Slackware update for proftpd - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>
Bug 2858 -- CVE-2006-5815: remote code execution in ProFTPD	CONFIRM	<a href="http://bugs.proftpd.org">bugs.proftpd.org</a>
Trustix update for openldap and proftpd - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>
SecurityTracker.com Archives - ProFTPD sreplace() Off-by-one Bug Lets Remote Users Execute Arbitrary Code	SECTRACK	<a href="http://securitytracker.com">securitytracker.com</a>
SecurityFocus	BUGTRAQ	<a href="http://www.securityfocus.com">www.securityfocus.com</a>
IBM X-Force Exchange	XF	<a href="http://exchange.ibm.com">exchange.ibm.com</a>
GLEG Ltd. - Information Security Company	MISC	<a href="http://gleg.net">gleg.net</a>

ProFTPD "sreplace()" Buffer Overflow Vulnerability - Advisories - Secunia	SECUNIA	<a href="https://secunia.com">secunia.co</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="https://www.vupez.com">www.vupez.com</a>
Mandriva update for proftpd - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	<a href="https://secunia.com">secunia.co</a>
Advisories - Mandriva Linux	MANDRIVA	<a href="https://www.mandriva.com">www.mandriva.com</a>
OpenPKG Meta: SiteMap	OPENPKG	<a href="https://www.openpkg.com">www.openpkg.com</a>
214820 – (CVE-2006-5815) CVE-2006-5815: proftpd unspecified vulnerability	CONFIRM	<a href="https://bugzilla.redhat.com">bugzilla.re</a>
Gentoo update for proftpd - Advisories - Secunia	SECUNIA	<a href="https://secunia.com">secunia.co</a>
ProFTPD SReplace Remote Buffer Overflow Vulnerability	BID	<a href="https://www.securityfocus.com">www.secu</a>
The Slackware Linux Project: Slackware Security Advisories	SLACKWARE	<a href="https://slackware.com">slackware</a>
Advisories - Mandriva Linux	MANDRIVA	<a href="https://www.mandriva.com">www.mandriva.com</a>
Debian update for proftpd - Advisories - Secunia	SECUNIA	<a href="https://secunia.com">secunia.co</a>
2006-0070	TRUSTIX	<a href="https://www.trustix.com">www.trust</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.o</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.g</a>



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). This site includes MITRE data granted under the following [license](https://mitre.org).

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