



# CVE-2006-5925

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

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2006-5925   |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | secalert@redhat.com   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2006-11-15 19:07:00 UTC   |
| <b>Updated</b>         | 2018-10-17 21:45:00 UTC   |
| <b>Description</b>     | Links web browser 1.00pre12 and Elinks 0.9.2 with smbclient installed allows remote attackers to execute arbitrary code via |

## 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="#">Elinks</a> | <a href="#">Elinks</a> | 0.9.2     | All    | All     | All      |
| Application | <a href="#">Elinks</a> | <a href="#">Elinks</a> | 0.9.2     | All    | All     | All      |
| Application | <a href="#">Links</a>  | <a href="#">Links</a>  | 1.00pre12 | All    | All     | All      |
| Application | <a href="#">Links</a>  | <a href="#">Links</a>  | 1.00pre12 | All    | All     | All      |

## References

| Reference   | Source   | Link   |
|---|----------|--|
| 2007-0005   | TRUSTIX  | <a href="http://www.trustix.org">www.trustix.org</a>                           |
| Mandriva update for links - Advisories - Secunia                                    | SECUNIA  | <a href="http://secunia.com">secunia.com</a>                                   |
| Security Announcement   | SUSE     | <a href="http://www.novell.com">www.novell.com</a>                             |
| SUSE Update for Multiple Packages - Advisories - Secunia                            | SECUNIA  | <a href="http://secunia.com">secunia.com</a>                                   |
| IBM X-Force Exchange  | XF       | <a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a> |
| Links SMB URL Parsing Bug Lets Remote Users Upload/Download Files - SecurityTracker | SECTRACK | <a href="http://securitytracker.com">securitytracker.com</a>                   |
| Trustix update for bind and ed - Advisories - Secunia                               | SECUNIA  | <a href="http://secunia.com">secunia.com</a>                                   |
| Debian -- Security Information -- DSA-1240-1 links2                                 | DEBIAN   | <a href="http://www.debian.org">www.debian.org</a>                             |
| Debian -- Security Information -- DSA-1226-1 links                                  | DEBIAN   | <a href="http://www.debian.org">www.debian.org</a>                             |
| Debian update for links2 - Advisories - Secunia                                     | SECUNIA  | <a href="http://secunia.com">secunia.com</a>                                   |

|  |          |   |
|--|----------|---|
| Debian update for elinks - Secunia Advisories - Vulnerability Intelligence - Secunia.com | SECUNIA  | <a href="https://secunia.com">secunia.com</a>                     |
| Gentoo update for elinks - Advisories - Secunia  | SECUNIA  | <a href="https://secunia.com">secunia.com</a>                     |
| Red Hat update for elinks - Advisories - Secunia   | SECUNIA  | <a href="https://secunia.com">secunia.com</a>                     |
| 403 Forbidden  | CONFIRM  | <a href="https://bugzilla.elinks.cz">bugzilla.elinks.cz</a>       |
| Gentoo update for links - Advisories - Secunia   | SECUNIA  | <a href="https://secunia.com">secunia.com</a>                     |
| Links "smb" Protocol File Upload/Download Vulnerability - Advisories - Secunia           | SECUNIA  | <a href="https://secunia.com">secunia.com</a>                     |
| Debian update for links - Advisories - Secunia   | SECUNIA  | <a href="https://secunia.com">secunia.com</a>                     |
| Repository / Oval Repository   | OVAL     | <a href="https://oval.cisecurity.org">oval.cisecurity.org</a>     |
| '[Full-disclosure] Links smbclient command execution' - MARC                             | FULLDISC | <a href="https://marc.info">marc.info</a>                         |
| <a href="https://rhn.redhat.com">rhn.redhat.com</a>   Red Hat Support                    | REDHAT   | <a href="https://www.redhat.com">www.redhat.com</a>               |
| ELinks SMB URL Parsing Bug Lets Remote Users Upload/Download Files - SecurityTracker     | SECTRACK | <a href="https://securitytracker.com">securitytracker.com</a>     |
| SecurityFocus  | BUGTRAQ  | <a href="https://www.securityfocus.com">www.securityfocus.com</a> |
| Links, ELinks 'smbclient' Remote Command Execution Vulnerability                         | BID      | <a href="https://www.securityfocus.com">www.securityfocus.com</a> |
| ELinks "smb" Protocol File Upload/Download Vulnerability - Advisories - Secunia          | SECUNIA  | <a href="https://secunia.com">secunia.com</a>                     |
| Advisories - Mandriva Linux  | MANDRIVA | <a href="https://www.mandriva.com">www.mandriva.com</a>           |
| Gentoo Linux Documentation -- ELinks: Arbitrary Samba command execution                  | GENTOO   | <a href="https://www.gentoo.org">www.gentoo.org</a>               |
| Debian -- Security Information -- DSA-1228-1 elinks                                      | DEBIAN   | <a href="https://www.debian.org">www.debian.org</a>               |
| Gentoo Linux Documentation -- Links: Arbitrary Samba command execution                   | GENTOO   | <a href="https://security.gentoo.org">security.gentoo.org</a>     |
| CVE Program record   | CVE.ORG  | <a href="https://www.cve.org">www.cve.org</a>                     |
| NVD vulnerability detail   | NVD      | <a href="https://nvd.nist.gov">nvd.nist.gov</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://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

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