



# CVE-2001-0441

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

## Summary

|                        |                                                                                                                              |
|------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2001-0441                                                                                                                |
| <b>State</b>           | PUBLIC                                                                                                                       |
| <b>Assigner</b>        | cve@mitre.org                                                                                                                |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                 |
| <b>Published</b>       | 2001-06-27 04:00:00 UTC                                                                                                      |
| <b>Updated</b>         | 2017-12-19 02:29:00 UTC                                                                                                      |
| <b>Description</b>     | Buffer overflow in (1) wrapping and (2) unwrapping functions of slrn news reader before 0.9.7.0 allows remote attackers to e |

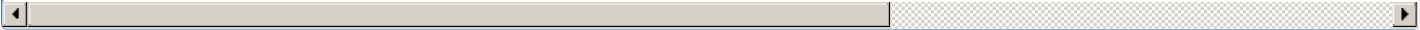
## Risk And Classification

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

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                       | Product                                         | Version | Update | Edition | Language |
|------------------|------------------------------|-------------------------------------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Debian</a>       | <a href="#">Debian Linux</a>                    | All     | All    | All     | All      |
| Operating System | <a href="#">Mandrakesoft</a> | <a href="#">Mandrake Linux</a>                  | 6.0     | All    | All     | All      |
| Operating System | <a href="#">Mandrakesoft</a> | <a href="#">Mandrake Linux</a>                  | 6.1     | All    | All     | All      |
| Operating System | <a href="#">Mandrakesoft</a> | <a href="#">Mandrake Linux</a>                  | 7.0     | All    | All     | All      |
| Operating System | <a href="#">Mandrakesoft</a> | <a href="#">Mandrake Linux</a>                  | 7.1     | All    | All     | All      |
| Operating System | <a href="#">Mandrakesoft</a> | <a href="#">Mandrake Linux</a>                  | 7.2     | All    | All     | All      |
| Operating System | <a href="#">Mandrakesoft</a> | <a href="#">Mandrake Linux</a>                  | 6.0     | All    | All     | All      |
| Operating System | <a href="#">Mandrakesoft</a> | <a href="#">Mandrake Linux</a>                  | 6.1     | All    | All     | All      |
| Operating System | <a href="#">Mandrakesoft</a> | <a href="#">Mandrake Linux</a>                  | 7.0     | All    | All     | All      |
| Operating System | <a href="#">Mandrakesoft</a> | <a href="#">Mandrake Linux</a>                  | 7.1     | All    | All     | All      |
| Operating System | <a href="#">Mandrakesoft</a> | <a href="#">Mandrake Linux</a>                  | 7.2     | All    | All     | All      |
| Operating System | <a href="#">Mandrakesoft</a> | <a href="#">Mandrake Linux Corporate Server</a> | 1.0.1   | All    | All     | All      |
| Operating System | <a href="#">Mandrakesoft</a> | <a href="#">Mandrake Linux Corporate Server</a> | 1.0.1   | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>       | <a href="#">Linux</a>                           | 6.2     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>       | <a href="#">Linux</a>                           | 7.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>       | <a href="#">Linux</a>                           | 6.2     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>       | <a href="#">Linux</a>                           | 7.0     | All    | All     | All      |

| References                                                                                                                     |       |
|--------------------------------------------------------------------------------------------------------------------------------|-------|
| Reference                                                                                                                      | Score |
| redhat.com   Red Hat Support                                                                                                   | RE    |
| MandrakeSoft Security Advisory MDKSA-2001:028 : slrn                                                                           | M/    |
| Home - Conectiva                                                                                                               | CC    |
| Debian -- Security Information -- DSA-040-1 slrn                                                                               | DE    |
| IBM X-Force Exchange                                                                                                           | XF    |
| 'Immunix OS Security update for slrn' - MARC                                                                                   | BL    |
| Neohapsis Archives - FreeBSD Security - FreeBSD Security Advisory FreeBSD-SA-01:37.slrn - From security-advisories@FreeBSD.org | FF    |
| SLRN Long Header Buffer Overflow Vulnerability                                                                                 | BI    |
| CVE Program record                                                                                                             | CV    |
| NVD vulnerability detail                                                                                                       | NV    |



No vendor comments have been submitted for this CVE.

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