



# CVE-2006-3015

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2006-3015  |
| <b>State</b>           | PUBLIC   |
| <b>Assigner</b>        | cve@mitre.org  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2006-06-14 15:06:00 UTC  |
| <b>Updated</b>         | 2017-07-20 01:31:00 UTC  |
| <b>Description</b>     | Argument injection vulnerability in WinSCP 3.8.1 build 328 allows remote attackers to upload or download arbitrary files via |

## Risk And Classification

### Problem Types: CWE-94

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                 | Product                | Version        | Update | Edition | Language |
|-------------|------------------------|------------------------|----------------|--------|---------|----------|
| Application | <a href="#">Winscp</a> | <a href="#">Winscp</a> | 3.8.1_build328 | All    | All     | All      |
| Application | <a href="#">Winscp</a> | <a href="#">Winscp</a> | 3.8.1_build328 | All    | All     | All      |

## References

| Reference  | Source   | Link   | Tags       |
|--|----------|--|------------|
| WinSCP URI Handler Remote Arbitrary File Access Vulnerability                | BID      | <a href="http://www.securityfocus.com">www.securityfocus.com</a>               | Exploit    |
| US-CERT Vulnerability Note VU#912588   | CERT-VN  | <a href="http://www.kb.cert.org">www.kb.cert.org</a>                           | US Govern  |
| WinSCP Protocol Handler Command Line Switch Injection - Advisories - Secunia | SECUNIA  | <a href="http://secunia.com">secunia.com</a>                                   | Vendor Ad  |
| Webmail - OVH  | VUPEN    | <a href="http://www.vupen.com">www.vupen.com</a>                               |            |
| 20060310 WinSCP - URI Handler Command Switch Parsing                         | FULLDISC | <a href="http://archives.neohapsis.com">archives.neohapsis.com</a>             |            |
| IBM X-Force Exchange   | XF       | <a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a> |            |
| [Full-disclosure] WinSCP - URI Handler Command Switch Parsing                | FULLDISC | <a href="http://lists.grok.org.uk">lists.grok.org.uk</a>                       | Exploit    |
| WinSCP :: Recent Version History   | CONFIRM  | <a href="http://winscp.net">winscp.net</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, |

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](#)**