



# CVE-2014-2735

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

## Summary

<b>CVE</b>	CVE-2014-2735
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2014-04-22 13:06:00 UTC
<b>Updated</b>	2018-10-09 19:43:00 UTC
<b>Description</b>	WinSCP before 5.5.3, when FTP with TLS is used, does not verify that the server hostname matches a domain name in the

## Risk And Classification

**Problem Types:** CWE-20

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Winscp	Winscp	5.5	All	All	All
Application	Winscp	Winscp	5.5.1	All	All	All
Application	Winscp	Winscp	5.5	All	All	All
Application	Winscp	Winscp	5.5.1	All	All	All
Application	Winscp	Winscp	All	All	All	All

## References

Reference	Source
SecurityFocus	BUGTRAQ
Recent Version History :: WinSCP	CONFIRM
Bug 1152 – Server hostname is not verified against certificate common name (or subject alternative name) :: Tracker :: WinSCP	CONFIRM
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#)