



CVE-2005-1583

Published on: 05/14/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:25 PM UTC

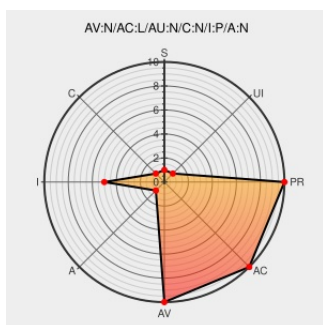
CVE-2005-1583

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [1two News](#) from [1two](#) contain the following vulnerability:

1Two News 1.0 allows remote attackers to (1) delete images for new stories via a direct request to admin/delete.php or (2) upload arbitrary images via a direct request to admin/upload.php.

CVE-2005-1583 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

**Access
Vector**

NETWORK

**Access
Complexity**

LOW

Authentication

NONE

**Confidentiality
Impact**

NONE

**Integrity
Impact**

PARTIAL

**Availability
Impact**

NONE

CVE References

Description

1Two News Lets Remote Users Delete Images, Upload Images, and Conduct Cross-Site Scripting Attacks - SecurityTracker

Tags

[Exploit](#)
[Patch](#)
[Vendor Advisory](#)
[securitytracker.com](#)
[text/html](#)

Link

[SECTRAK 1013960](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	1two	1two News	1.0	All	All	All
Application	1two	1two News	1.0	All	All	All
cpe:2.3:a:1two:1two_news:1.0:*****::						
cpe:2.3:a:1two:1two_news:1.0:*****::						
No vendor comments have been submitted for this CVE						
← Previous ID				Next ID→		