



CVE-2006-0371

Published on: 01/22/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:07 PM UTC

CVE-2006-0371

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Rcblog](#) from [Noah Medling](#) contain the following vulnerability:

Directory traversal vulnerability in index.php in Noah Medling RCBlog 1.03 allows remote attackers to read arbitrary .txt files, possibly including one that stores the administrator's account name and password, via a .. (dot dot) in the post parameter.

CVE-2006-0371 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

PARTIAL

Integrity
Impact

NONE

Availability
Impact

NONE

CVE References

Description

Tags

Link

SecurityFocus

www.securityfocus.com
text/html

[BUGTRAQ 20060218 RCBlog exploit \[fun\]](#)

SecurityFocus

www.securityfocus.com
text/html

[BUGTRAQ 20060611 RCBlog 1.03 Directory Traversal \[index.php\]](#)

RCBlog Index.PHP Directory Traversal Vulnerability

[Exploit](#)
[cve.report \(archive\)](#)
text/html

[BID 16342](#)

IBM X-Force Exchange

exchange.xforce.ibmcloud.com
text/html

[XF rcblog-index-directory-traversal\(24248\)](#)

RCBlog File Upload and Disclosure of Sensitive Information - Advisories - Secunia

[Vendor Advisory](#)
web.archive.org
text/html

[SECUNIA 18547](#)

SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20060120 [eVuln] RCBlog Directory Traversal & Sensitive Information Disclosure
RCBlog - Fluffington.com	www.fluffington.com text/html	MISC www.fluffington.com/index.php?page=rcblog
eVuln.com - RCBlog Directory Traversal & Sensitive Information Disclosure	Exploit Vendor Advisory evuln.com text/html	MISC evuln.com/vulns/42/summary.html
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 22680
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF rcblog-index-file-include(27042)
SecurityTracker.com Archives - RCBlog Input Validation Hole Lets Remote Users Traverse the Directory	securitytracker.com text/html	SECTRAK 1015523
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	Noah Medling	Rcblog	1.03	All	All	All
Application	Noah Medling	Rcblog	1.03	All	All	All
<code>cpe:2.3:a:noah_medling:rcblog:1.03:*****:*</code>						
<code>cpe:2.3:a:noah_medling:rcblog:1.03:*****:*</code>						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023 |

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](#)