



CVE-2010-0667

Published on: 02/26/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:06 PM UTC

CVE-2010-0667

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

Certain versions of [Moinmoin](#) from [Moinmo](#) contain the following vulnerability:

MoinMoin 1.9 before 1.9.1 does not perform the expected clearing of the sys.argv array in situations where the GATEWAY_INTERFACE environment variable is set, which allows remote attackers to obtain sensitive information via unspecified vectors.

CVE-2010-0667 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

MoinMoin "sys.argv" Information Disclosure Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com

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

[X](#) [SECUNIA 38242](#)

SecurityFixes - MoinMoin

[Vendor Advisory](#)
[moinmo.in](#)
[text/html](#)

[M](#) [CONFIRM moinmo.in/SecurityFixes](#)

oss-security - CVE Request -- MoinMoin -- 1.8.7

[www.openwall.com](#)
[text/html](#)

[O](#) [MLIST \[oss-security\] 20100215 CVE Request -- MoinMoin -- 1.8.7](#)

'[oss-security] Re: CVE Request -- MoinMoin -- 1.8.7' - MARC

[marc.info](#)
[text/html](#)

[G](#) [MLIST \[oss-security\] 20100221 Re: CVE Request -- MoinMoin -- 1.8.7](#)

oss-security - CVE request: MoinMoin information disclosure

[www.openwall.com](#)
[text/html](#)

[O](#) [MLIST \[oss-security\] 20100121 CVE request: MoinMoin information disclosure](#)

'[oss-security] Re: CVE Request -- MoinMoin -- 1.8.7' - MARC	marc.info text/html	MLIST [oss-security] 20100215 Re: CVE Request -- MoinMoin -- 1.8.7
MoinMoinChat/Logs/moin-dev/2010-01-18 - MoinMoin	moinmo.in text/html	CONFIRM moinmo.in/MoinMoinChat/Logs/moin-dev/2010-01-18
502 Bad Gateway	hg.moinmo.in text/plain Inactive Link Not Archived	CONFIRM hg.moinmo.in/moin/1.9/raw-file/1.9.1/docs/CHANGES
moin/1.9: changeset 5461:9d8e7ce3c3a2	web.archive.org text/xml Inactive Link Not Archived	CONFIRM hg.moinmo.in/moin/1.9/rev/9d8e7ce3c3a2
moin/1.9: changeset 5459:04afdde50094	web.archive.org text/xml Inactive Link Not Archived	CONFIRM hg.moinmo.in/moin/1.9/rev/04afdde50094

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	Moinmo	Moinmoin	1.9.0	All	All	All
Application	Moinmo	Moinmoin	1.9.0	All	All	All
cpe:2.3:a:moinmo:moinmoin:1.9.0:*:*:*:*:*:						
cpe:2.3:a:moinmo:moinmoin:1.9.0:*:*:*:*:*:						

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](#)