

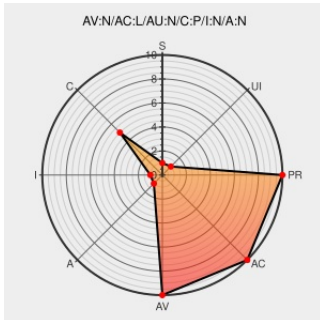


CVE-2007-4960

Published on: 09/18/2007 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:32 PM UTC

CVE-2007-4960

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

Certain versions of [Second Life](#) from [Linden Lab](#) contain the following vulnerability:

Argument injection vulnerability in the Linden Lab Second Life secondlife:// protocol handler, as used in Internet Explorer and possibly Firefox, allows remote attackers to obtain sensitive information via a "" (double-quote space) sequence followed by the -autologin and -loginuri arguments, which cause the handler to post login credentials and software installation details to an arbitrary URL.

CVE-2007-4960 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20070916 IE (Internet Explorer) pwns SecondLife
IE pwns SecondLife GNUCITIZEN	www.gnucitizen.org text/html	MISC www.gnucitizen.org/blog/ie-pwns-secondlife
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2007-3188
Second Life URI Handler Registration Vulnerability - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 26845
IBM X-Force Exchange	exchange.xforce.ibmcloud.com	XF secondlife-secondlife-info-

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	Linden Lab	Second Life	1	All	All	All
Application	Linden Lab	Second Life	1	All	All	All
cpe:2.3:a:linden_lab:second_life:1:*:*:*:*:*:						
cpe:2.3:a:linden_lab:second_life:1:*:*:*:*:*:						

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](#)