

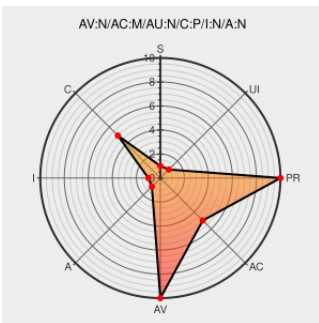


CVE-2005-2095

Published on: 07/13/2005 12:00:00 AM UTC

Last Modified on: 02/13/2023 01:09:26 AM UTC

CVE-2005-2095

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

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

options_identities.php in SquirrelMail 1.4.4 and earlier uses the extract function to process the \$_POST variable, which allows remote attackers to modify or read the preferences of other users, conduct cross-site scripting (XSS) attacks, and write arbitrary files.

CVE-2005-2095 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

NETWORK

MEDIUM

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

PARTIAL

NONE

NONE

CVE References

Description

Tags

Link

SecurityFocus

www.securityfocus.com
text/html

[BUGTRAQ 20050714 SquirrelMail Arbitrary Variable Overwriting Vulnerability](#)

IBM X-Force Exchange

exchange.xforce.ibmcloud.com
text/html

[XF squirrelmail-set-post-variable\(21359\)](#)

Support

www.redhat.com
text/html

[REDHAT RHSA-2005:595](#)

Debian -- Security Information -- DSA-756-1
squirrelmail

[Patch](#)
[Vendor Advisory](#)
www.debian.org
[Deprecated Link](#)
text/html

[DEBIAN DSA-756](#)

Contact Support

www.gulftech.org
text/html

[MISC www.gulftech.org/?node=research&article_id=00090-07142005](#)

SquirrelMail - Webmail for Nuts!	www.squirrelmail.org text/html	 CONFIRM www.squirrelmail.org/security/issue/2005-07-13
163047 – CAN-2005-1769,2095 Multiple XSS issues in squirrelmail	bugzilla.redhat.com text/html	 FEDORA FLSA:163047
SquirrelMail Variable Handling Vulnerability	cve.report (archive) text/html	 BID 14254
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval.org.mitre.oval:def:10500
SecurityFocus	www.securityfocus.com text/html	 BUGTRAQ 20050714 [SM-ANNOUNCE] Patch available for CAN-2005-2095
Security Announcement	web.archive.org text/html Inactive Link Not Archived	 SUSE SUSE-SR:2005:018
APPLE-SA-2005-08-17 Security Update 2005-007 v1.1	lists.apple.com text/html	 APPLE APPLE-SA-2005-08-17
APPLE-SA-2005-08-15 Security Update 2005-007	lists.apple.com text/html	 APPLE APPLE-SA-2005-08-15
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	Squirrelmail	Squirrelmail	1.0.4	All	All	All
Application	Squirrelmail	Squirrelmail	1.0.5	All	All	All
Application	Squirrelmail	Squirrelmail	1.2.0	All	All	All
Application	Squirrelmail	Squirrelmail	1.2.1	All	All	All
Application	Squirrelmail	Squirrelmail	1.2.10	All	All	All
Application	Squirrelmail	Squirrelmail	1.2.11	All	All	All
Application	Squirrelmail	Squirrelmail	1.2.2	All	All	All
Application	Squirrelmail	Squirrelmail	1.2.3	All	All	All
Application	Squirrelmail	Squirrelmail	1.2.4	All	All	All
Application	Squirrelmail	Squirrelmail	1.2.5	All	All	All
Application	Squirrelmail	Squirrelmail	1.2.6	All	All	All
Application	Squirrelmail	Squirrelmail	1.2.7	All	All	All
Application	Squirrelmail	Squirrelmail	1.2.8	All	All	All
Application	Squirrelmail	Squirrelmail	1.2.9	All	All	All

cpe:2.3:a:squirrelmail:squirrelmail:1.2.10:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.2.11:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.2.2:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.2.3:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.2.4:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.2.5:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.2.6:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.2.7:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.2.8:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.2.9:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.4:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.4.0:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.4.1:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.4.2:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.4.3:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.4.3a:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.4.3_rc1:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.44:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.0.4:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.0.5:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.2.0:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.2.1:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.2.10:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.2.11:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.2.2:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.2.3:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.2.4:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.2.5:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.2.6:*****:

cpe:2.3:a:squirrelmail:squirrelmail:1.2.7:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.2.8:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.2.9:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.4:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.4.0:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.4.1:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.4.2:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.4.3:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.4.3a:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.4.3_rc1:*****:
cpe:2.3:a:squirrelmail:squirrelmail:1.44:*****:

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](#)