

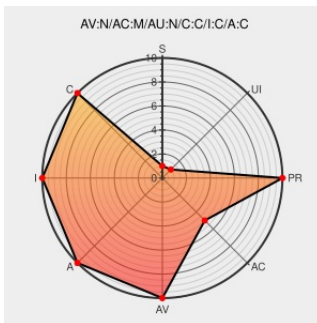


CVE-2005-1924

Published on: 12/31/2005 05:00:00 AM UTC

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

CVE-2005-1924

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

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

The G/PGP (GPG) Plugin 2.1 and earlier for Squirrelmail allow remote authenticated users to execute arbitrary commands via shell metacharacters in (1) the fpr parameter to the deleteKey function in gpg_keyring.php, as called by (a) import_key_file.php, (b) import_key_text.php, and (c) keyring_main.php; and (2) the keyserver parameter to the gpg_recv_key function in gpg_key_functions.php, as called by gpg_options.php. NOTE: this issue may overlap CVE-2007-3636.

CVE-2005-1924 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **9.3 - HIGH**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Gentoo Linux Documentation -- SquirrelMail G/PGP plugin: Arbitrary code execution

[security.gentoo.org](#)
[text/html](#)

[GENTOO GLSA-200708-08](#)

SquirrelMail G/PGP Encryption Plug-in Multiple Remote Command Execution Vulnerabilities

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

[BID 24874](#)

[VIM] True: SquirrelMail G/PGP Encryption Plug-in 2.0 Command Execution Vuln

[www.attrition.org](#)
[text/html](#)

[VIM 20070711 True: SquirrelMail G/PGP Encryption Plug-in 2.0 Command Execution Vuln](#)

SecurityFocus

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

[BUGTRAQ 20070711 SquirrelMail G/PGP Encryption Plug-in Remote Command Execution Vulnerability](#)

No Description Provided	web.archive.org text/html Inactive Link Not Archived	IDEFENSE 20070711 SquirrelMail G/PGP Plugin deleteKey() Command Injection Vulnerability
No Description Provided	osvdb.org Inactive Link Not Archived	OSVDB 37924
No Description Provided	osvdb.org Inactive Link Not Archived	OSVDB 37923
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF squirrelmail-gpgp-keyfunc-command-execution(35364)
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2007-2513
SquirrelMail G/PGP Encryption Plugin Multiple Vulnerabilities - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 26035
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF squirrelmail-gpgp-keyring-command-execution(35355)
Gentoo update for squirrelmail - Advisories - Secunia	web.archive.org text/html	SECUNIA 26424
SquirrelMail G/PGP Encryption Plug-in 2.0 Command Execution Vuln	www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 4173
No Description Provided	web.archive.org text/html Inactive Link Not Archived	IDEFENSE 20070711 SquirrelMail G/PGP Plugin pgp_recv_key() Command Injection Vulnerability

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	Gpg Plugin	All	All	All	All
cpe:2.3:a:squirrelmail:gpg_plugin:*****:*						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)