



CVE-2017-7692

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2017-7692
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-20 14:59:00 UTC
Updated	2025-04-20 01:37:25 UTC
Description	SquirrelMail 1.4.22 (and other versions before 20170427_0200-SVN) allows post-authentication remote code execution via

Risk And Classification

Primary CVSS: v3.0 8.8 HIGH from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Problem Types: CWE-20 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	9		AV:N/AC:L/Au:S/C:C/I:C/A:C

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:L/Au:S/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Squirrelmail	Squirrelmail	1.4.22	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference

SquirrelMail-Exploit-Remote-Code-Exec-CVE-2017-7692-Vuln

Squirrelmail CVE-2017-7692 Command Injection Vulnerability

SquirrelMail Input Validation Flaw in 'Deliver_SendMail.class.php' Lets Remote Authenticated Users Execute Arbitrary Commands on the Target

oss-security - CVE-2017-7692: Squirrelmail 1.4.22 Remote Code Execution

SquirrelMail < 1.4.22 - Remote Code Execution

oss-security - Re: SquirrelMail <= 1.4.23 Remote Code Execution (CVE-2017-7692)

SquirrelMail: Remote Code Execution (GLSA 201709-13) — Gentoo security

Debian -- Security Information -- DSA-3852-1 squirrelmail

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)