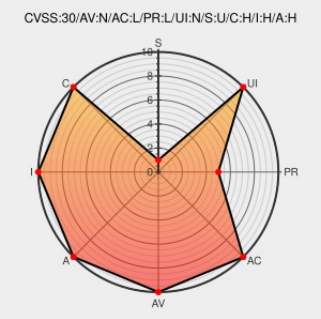
CVE-2018-8741

Published on: 03/17/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:41 PM UTC

CVE-2018-8741

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Debian Linux from Debian contain the following vulnerability:

A directory traversal flaw in SquirrelMail 1.4.22 allows an authenticated attacker to exfiltrate (or potentially delete) files from the hosting server, related to ../ in the att_local_name field in Deliver.class.php.

CVE-2018-8741 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
squirrelmail quick fix for file disclosure vuln presented at Troopers 2018 (#TR18) · GitHub	Patch Third Party Advisory gist.github.com text/html	MISC gist.github.com/hannob/3c4f86863c418930ad08853c1109364e

SquirrelMail Input Validation Flaw in 'Deliver.class.php' Lets Remote Authenticated Users View Files on the Target System - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1040554
[SECURITY] Fedora 29 Update: squirrelmail-1.4.23-1.fc29.20190710 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2019-1a87523729
[SECURITY] Fedora 30 Update: squirrelmail-1.4.23-1.fc30.20190710 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2019-ad02f64a79
Squirrelmail Full Disclosure – TROOPERS18 – Insinuator.net	Patch Third Party Advisory insinuator.net text/html	MISC insinuator.net/2018/03/squirrelmail-full-disclosure-troopers18/
Paste #OjSLiFTxiBrTk63jqEUu at spacepaste	Third Party Advisory paste.pound-python.org text/html	MISC paste.pound-python.org/show/OjSLiFTxiBrTk63jqEUu/
Debian -- Security Information -- DSA-4168-1 squirrelmail	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-4168
[SECURITY] [DLA 1344-1] squirrelmail security update	Mailing List Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20180416 [SECURITY] [DLA 1344-1] squirrelmail security update
oss-security - Squirrelmail directory traversal vulnerability allows exfiltrating files from server	Mailing List Third Party Advisory www.openwall.com text/html	MISC www.openwall.com/lists/oss-security/2018/03/17/2

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Squirrelmail	Squirrelmail	1.4.22	All	All	All
Application	Squirrelmail	Squirrelmail	1.4.22	All	All	All

cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:*

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*

cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:*

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*

cpe:2.3:a:squirrelmail:squirrelmail:1.4.22:*:*:*:*:*:*:*

cpe:2.3:a:squirrelmail:squirrelmail:1.4.22:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→