



CVE-2019-13122

Published on: 07/10/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:46 PM UTC

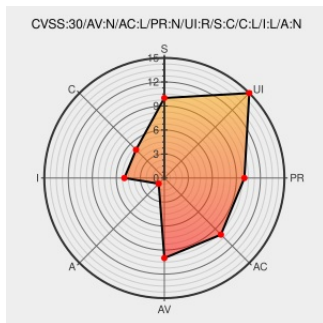
CVE-2019-13122

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

A Cross Site Scripting (XSS) vulnerability exists in the template tag used to render message ids in Patchwork v1.1 through v2.1.x. This allows an attacker to insert JavaScript or HTML into the patch detail page via an email sent to a mailing list consumed by Patchwork. This affects the function msgid in templatetags/patch.py. Patchwork versions v2.1.4 and v2.0.4 will contain the fix.

CVE-2019-13122 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
oss-security - CVE-2019-13122: Patchwork: XSS via Message-ID	Mailing List Third Party Advisory	MLIST [oss-security] 20190705 CVE-2019-13122: Patchwork: XSS via Message-ID

	www.openwall.com text/html	
[PATCH 0/2] XSS in Patchwork - CVE-2019-13122	Mailing List Vendor Advisory lists.ozlabs.org text/html	 MISC lists.ozlabs.org/pipermail/patchwork/2019-July/005870.html
Releases · getpatchwork/patchwork · GitHub	Release Notes Third Party Advisory github.com text/html	 MISC github.com/getpatchwork/patchwork/releases
[PATCH] docs: Add a release note for CVE-2019-13122	Mailing List Vendor Advisory lists.ozlabs.org text/html	 MISC lists.ozlabs.org/pipermail/patchwork/2019-July/005878.html
Commits · getpatchwork/patchwork · GitHub	Third Party Advisory github.com text/html	 MISC github.com/getpatchwork/patchwork/commits/master
The Patchwork July 2019 Archive by date	Vendor Advisory lists.ozlabs.org text/html	 MISC lists.ozlabs.org/pipermail/patchwork/2019-July/date.html
patchwork	Vendor Advisory jk.ozlabs.org text/html	 MISC jk.ozlabs.org/projects/patchwork/

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.

Related QID Numbers

501221 Alpine Linux Security Update for patchwork

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ozlabs	Patchwork	All	All	All	All
Application	Ozlabs	Patchwork	2.1.0	rc1	All	All
Application	Ozlabs	Patchwork	2.1.0	rc2	All	All
Application	Ozlabs	Patchwork	All	All	All	All
Application	Ozlabs	Patchwork	2.1.0	rc1	All	All
Application	Ozlabs	Patchwork	2.1.0	rc2	All	All
cpe:2.3:a:ozlabs:patchwork:*****:						
cpe:2.3:a:ozlabs:patchwork:2.1.0:rc1:*****:						
cpe:2.3:a:ozlabs:patchwork:2.1.0:rc2:*****:						
cpe:2.3:a:ozlabs:patchwork:*****:						

cpe:2.3:a:ozlabs:patchwork:2.1.0:rc1:****:*:

cpe:2.3:a:ozlabs:patchwork:2.1.0:rc2:****:*:

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](#)