



CVE-2021-35525

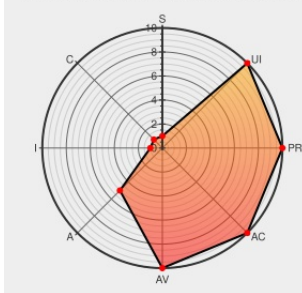
Published on: 06/28/2021 12:00:00 AM UTC

Last Modified on: 09/20/2021 06:52:00 PM UTC

CVE-2021-35525

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

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L



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

PostSRSD before 1.11 allows a denial of service (subprocess hang) if Postfix sends certain long data fields such as multiple concatenated email addresses. NOTE: the PostSRSD maintainer acknowledges "theoretically, this error should never occur ... I'm not sure if there's a reliable way to trigger this condition by an external attacker, but it is a security bug in PostSRSD nevertheless."

CVE-2021-35525 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.3 - MEDIUM**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
PostSRSD: Denial of service (GLSA 202107-08) —	security.gentoo.org text/html	GENTOO GLSA-202107-08

Gentoo security

SECURITY: Fix DoS on overly long input from Postfix · roehling/postersd@077be98 · GitHub

github.com

text/html

MISC

github.com/roehling/postersd/commit/077be98d8c8a9847e4ae0c7dc09e7474cbe27db2

793674 –

bugs.gentoo.org

text/html

MISC

bugs.gentoo.org/793674

Release 1.11 · roehling/postersd · GitHub

github.com

text/html

MISC

github.com/roehling/postersd/releases/tag/1.11

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

180583

Debian Security Update for postersd (CVE-2021-35525)

710068

Gentoo Linux PostSRSd Denial of service (GLSA 202107-08)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Postersd Project	Postersd	All	All	All	All
cpe:2.3:a:postersd_project:postersd:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-35525 : PostSRSd before 1.11 allows a denial of service subprocess hang if Postfix sends certain long da... twitter.com/i/web/status/1...	2021-06-28 18:02:55
/r/netcve	CVE-2021-35525	2021-06-28 18:41:29

← 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](#)