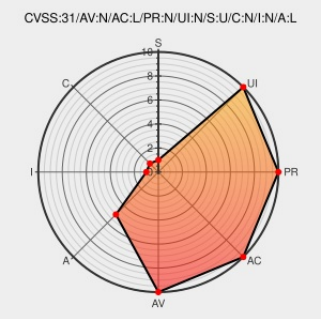
CVE-2021-35525

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



Certain versions of Postsrsd from Postsrsd 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 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/postsrsd@077be98 · GitHub	github.com text/html	MISC github.com/roehling/postsrsd/commit/077be98d8c8a9847e4ae0c7dc09e7474cbe27db2
793674 –	bugs.gentoo.org text/html	MISC bugs.gentoo.org/793674
Release 1.11 · roehling/postsrsd · GitHub	github.com text/html	MISC github.com/roehling/postsrsd/releases/tag/1.11

Related QID Numbers

180583 Debian Security Update for postsrsd (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	Postsrsd Project	Postsrsd	All	All	All	All

cpe:2.3:a:postsrsd_project:postsrsd:*:*:*:*:*:*:*:*:

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→