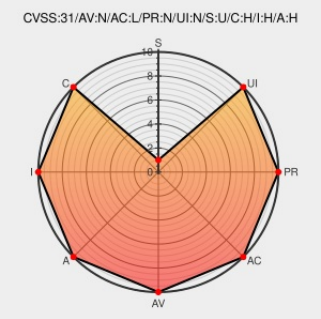
CVE-2020-12870

Published on: 09/30/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:36 PM UTC

CVE-2020-12870

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



Certain versions of Pacsone Server from Rainbowfishsoftware contain the following vulnerability:

RainbowFish PacsOne Server 6.8.4 allows SQL injection on the username parameter in the signup page.

CVE-2020-12870 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
PacsOne Server - Download	Release Notes, Vendor Advisory, www.pacsone.net, text/html	MISC www.pacsone.net/download.htm

cve-pocs/CVE-2020-12870 at master · bzyo/cve-pocs · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/bzyo/cve-pocs/tree/master/CVE-2020-12870

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rainbowfishsoftware	Pacsone Server	6.8.4	All	All	All
Application	Rainbowfishsoftware	Pacsone Server	6.8.4	All	All	All

cpe:2.3:a:rainbowfishsoftware:pacsone_server:6.8.4:*:*:*:*:*:*:*:

cpe:2.3:a:rainbowfishsoftware:pacsone_server:6.8.4:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→