



RainyGao DocSys getUserList.do getUserList sql injection

- [MITRE](#)
- [NVD](#)
- [CVE.ORG](#)
- [JSON API](#)
- [Print: PDF](#)

Summary	
CVE	CVE-2025-11629
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-10-12 07:15:43 UTC
Updated	2026-04-29 01:00:01 UTC
Description	A vulnerability has been found in RainyGao DocSys up to 2.02.36. This impacts the function getUserList of the file /Manage

Risk And Classification					
Primary CVSS: v4.0 2.1 LOW from cna@vulldb.com					
CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X					
Problem Types: CWE-74 CWE-89 CWE-89 SQL Injection CWE-74 Injection					
Version	Source	Type	Score	Severity	Vector
4.0	cna@vulldb.com	Secondary	2.1	LOW	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	DECLARED	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	cna@vulldb.com	Secondary	6.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	DECLARED	6.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:R
3.0	CNA	DECLARED	6.3	MEDIUM	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:R
2.0	cna@vulldb.com	Secondary	6.5		AV:N/AC:L/Au:S/C:P/I:P/A:P
2.0	CNA	DECLARED	6.5		AV:N/AC:L/Au:S/C:P/I:P/A:P/E:POC/RL:ND/RC:UR

CVSS v4.0 Breakdown	
Attack Vector	Network
Attack Complexity	Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X



CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:R

NVD Known Affected Configurations (CPE 2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Docsys Project	Docsys	All	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	RainyGao	DocSys	affected 2.02.0	Not specified
CNA	RainyGao	DocSys	affected 2.02.1	Not specified
CNA	RainyGao	DocSys	affected 2.02.2	Not specified
CNA	RainyGao	DocSys	affected 2.02.3	Not specified
CNA	RainyGao	DocSys	affected 2.02.4	Not specified
CNA	RainyGao	DocSys	affected 2.02.5	Not specified
CNA	RainyGao	DocSys	affected 2.02.6	Not specified
CNA	RainyGao	DocSys	affected 2.02.7	Not specified
CNA	RainyGao	DocSys	affected 2.02.8	Not specified
CNA	RainyGao	DocSys	affected 2.02.9	Not specified
CNA	RainyGao	DocSys	affected 2.02.10	Not specified
CNA	RainyGao	DocSys	affected 2.02.11	Not specified
CNA	RainyGao	DocSys	affected 2.02.12	Not specified
CNA	RainyGao	DocSys	affected 2.02.13	Not specified
CNA	RainyGao	DocSys	affected 2.02.14	Not specified
CNA	RainyGao	DocSys	affected 2.02.15	Not specified

CNA	RainyGao	DocSys	affected 2.02.16	Not specified
CNA	RainyGao	DocSys	affected 2.02.17	Not specified
CNA	RainyGao	DocSys	affected 2.02.18	Not specified
CNA	RainyGao	DocSys	affected 2.02.19	Not specified
CNA	RainyGao	DocSys	affected 2.02.20	Not specified
CNA	RainyGao	DocSys	affected 2.02.21	Not specified
CNA	RainyGao	DocSys	affected 2.02.22	Not specified
CNA	RainyGao	DocSys	affected 2.02.23	Not specified
CNA	RainyGao	DocSys	affected 2.02.24	Not specified
CNA	RainyGao	DocSys	affected 2.02.25	Not specified
CNA	RainyGao	DocSys	affected 2.02.26	Not specified
CNA	RainyGao	DocSys	affected 2.02.27	Not specified
CNA	RainyGao	DocSys	affected 2.02.28	Not specified
CNA	RainyGao	DocSys	affected 2.02.29	Not specified
CNA	RainyGao	DocSys	affected 2.02.30	Not specified
CNA	RainyGao	DocSys	affected 2.02.31	Not specified
CNA	RainyGao	DocSys	affected 2.02.32	Not specified
CNA	RainyGao	DocSys	affected 2.02.33	Not specified
CNA	RainyGao	DocSys	affected 2.02.34	Not specified
CNA	RainyGao	DocSys	affected 2.02.35	Not specified
CNA	RainyGao	DocSys	affected 2.02.36	Not specified

References

Reference	Source	Link
vuldb.com	cna@vuldb.com	vuldb.com
github.com/xkalami-Tta0/CVE/blob/main/DocSys/sql%E6%B3%A8%E5%85%A5.md	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
vuldb.com	cna@vuldb.com	vuldb.com
vuldb.com	cna@vuldb.com	vuldb.com
CVE Program record	CVE.ORG	www.cve.c
NVD vulnerability detail	NVD	nvd.nist.gc

Vendor Comments And Credit

Discovery Credit

CNA: Tta0 (VulDB User) (en)

Additional Advisory Data

Additional Advisory Data		
Source	Time	Event
CNA	2025-10-11T00:00:00.000Z	Advisory disclosed
CNA	2025-10-11T02:00:00.000Z	VulDB entry created
CNA	2025-10-11T15:56:18.000Z	VulDB entry last update
There are currently no legacy QID mappings associated with this CVE.		

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)