



CVE-2017-2255

Published on: 08/28/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:53 PM UTC

CVE-2017-2255

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

Certain versions of [Garoon](#) from [Cybozu](#) contain the following vulnerability:

Cross-site scripting vulnerability in Cybozu Garoon 3.7.0 to 4.2.5 allows an attacker to inject arbitrary web script or HTML via "Rich text" function of the application "Space".

CVE-2017-2255 has been assigned by [vultures@jpcert.or.jp](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [Cybozu, Inc.](#) - **Cybozu Garoon** version **3.7.0 to 4.2.5**

CVSS3 Score: **5.4 - MEDIUM**

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

CVSS2 Score: **3.5 - LOW**

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

CVE References

Description	Tags	Link
不具合情報公開サイト	Vendor Advisory support.cybozu.com text/html	CONFIRM support.cybozu.com/ja-jp/article/9746

text/html

JVN#63564682: Multiple vulnerabilities in Cybozu Garoon

Third Party Advisory

 JVN JVN#63564682

VDB Entry

jvn.jp

text/xml

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cybozu	Garoon	3.7.0	All	All	All
Application	Cybozu	Garoon	3.7.1	All	All	All
Application	Cybozu	Garoon	3.7.2	All	All	All
Application	Cybozu	Garoon	3.7.3	All	All	All
Application	Cybozu	Garoon	3.7.4	All	All	All
Application	Cybozu	Garoon	3.7.5	All	All	All
Application	Cybozu	Garoon	4.0.1	All	All	All
Application	Cybozu	Garoon	4.0.2	All	All	All
Application	Cybozu	Garoon	4.0.3	All	All	All
Application	Cybozu	Garoon	4.2.0	All	All	All
Application	Cybozu	Garoon	4.2.1	All	All	All
Application	Cybozu	Garoon	4.2.2	All	All	All
Application	Cybozu	Garoon	4.2.3	All	All	All
Application	Cybozu	Garoon	4.2.4	All	All	All
Application	Cybozu	Garoon	4.2.5	All	All	All
Application	Cybozu	Garoon	3.7.0	All	All	All
Application	Cybozu	Garoon	3.7.1	All	All	All
Application	Cybozu	Garoon	3.7.2	All	All	All
Application	Cybozu	Garoon	3.7.3	All	All	All
Application	Cybozu	Garoon	3.7.4	All	All	All
Application	Cybozu	Garoon	3.7.5	All	All	All
Application	Cybozu	Garoon	4.0.1	All	All	All
Application	Cybozu	Garoon	4.0.2	All	All	All
Application	Cybozu	Garoon	4.0.3	All	All	All
Application	Cybozu	Garoon	4.2.0	All	All	All

Application	Cybozu	Garoon	4.2.0	All	All	All
Application	Cybozu	Garoon	4.2.1	All	All	All
Application	Cybozu	Garoon	4.2.2	All	All	All
Application	Cybozu	Garoon	4.2.3	All	All	All
Application	Cybozu	Garoon	4.2.4	All	All	All
Application	Cybozu	Garoon	4.2.5	All	All	All
cpe:2.3:a:cybozu:garoon:3.7.0:*****:.*						
cpe:2.3:a:cybozu:garoon:3.7.1:*****:.*						
cpe:2.3:a:cybozu:garoon:3.7.2:*****:.*						
cpe:2.3:a:cybozu:garoon:3.7.3:*****:.*						
cpe:2.3:a:cybozu:garoon:3.7.4:*****:.*						
cpe:2.3:a:cybozu:garoon:3.7.5:*****:.*						
cpe:2.3:a:cybozu:garoon:4.0.1:*****:.*						
cpe:2.3:a:cybozu:garoon:4.0.2:*****:.*						
cpe:2.3:a:cybozu:garoon:4.0.3:*****:.*						
cpe:2.3:a:cybozu:garoon:4.2.0:*****:.*						
cpe:2.3:a:cybozu:garoon:4.2.1:*****:.*						
cpe:2.3:a:cybozu:garoon:4.2.2:*****:.*						
cpe:2.3:a:cybozu:garoon:4.2.3:*****:.*						
cpe:2.3:a:cybozu:garoon:4.2.4:*****:.*						
cpe:2.3:a:cybozu:garoon:4.2.5:*****:.*						
cpe:2.3:a:cybozu:garoon:3.7.0:*****:.*						
cpe:2.3:a:cybozu:garoon:3.7.1:*****:.*						
cpe:2.3:a:cybozu:garoon:3.7.2:*****:.*						
cpe:2.3:a:cybozu:garoon:3.7.3:*****:.*						
cpe:2.3:a:cybozu:garoon:3.7.4:*****:.*						
cpe:2.3:a:cybozu:garoon:3.7.5:*****:.*						
cpe:2.3:a:cybozu:garoon:4.0.1:*****:.*						
cpe:2.3:a:cybozu:garoon:4.0.2:*****:.*						
cpe:2.3:a:cybozu:garoon:4.0.3:*****:.*						

cpe:2.3:a:cybozu:garoon:4.2.0:*****:
cpe:2.3:a:cybozu:garoon:4.2.1:*****:
cpe:2.3:a:cybozu:garoon:4.2.2:*****:
cpe:2.3:a:cybozu:garoon:4.2.3:*****:
cpe:2.3:a:cybozu:garoon:4.2.4:*****:
cpe:2.3:a:cybozu:garoon:4.2.5:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)