

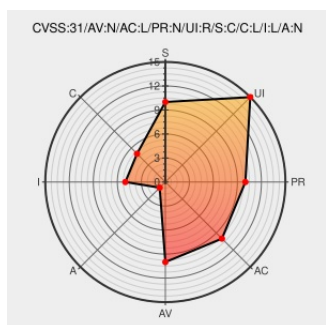


CVE-2020-5568

Published on: 04/27/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:03 PM UTC

CVE-2020-5568

[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 4.6.0 to 5.0.0 allows remote attackers to inject arbitrary web script or HTML via the applications 'Messages' and 'Bulletin Board'.

CVE-2020-5568 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 **4.6.0 to 5.0.0**

CVSS3 Score: **6.1 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
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 kb.cybozu.support text/html	MISC kb.cybozu.support/article/36302/

