



CVE-2020-5586

Published on: 06/30/2020 12:00:00 AM UTC

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

CVE-2020-5586

[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 4.10.3 to 5.0.1 allows attacker with administrator rights to inject an arbitrary script via unspecified vectors.

CVE-2020-5586 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 **4.10.3 to 5.0.1**

CVSS3 Score: **4.8 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	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
JVN#55497111: Multiple vulnerabilities in Cybozu Garoon	Third Party Advisory jvn.jp text/xml	MISC jvn.jp/en/jp/JVN55497111/index.html

