



Published on: 05/17/2019 12:00:00 AM UTC

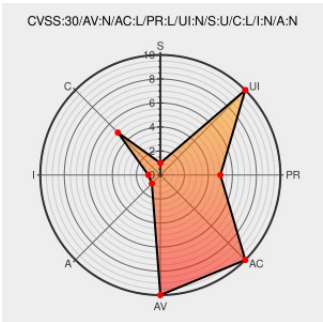
Last Modified on: 03/23/2021 11:27:59 PM UTC

CVE-2019-5942

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

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

Cybozu Garoon 4.0.0 to 4.10.1 allows remote authenticated attackers to bypass access restriction to obtain files without access privileges via the Multiple Files Download function of application 'Cabinet'.

CVE-2019-5942 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 4.0.0 to 4.10.1

CVSS3 Score: 4.3 - MEDIUM

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

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
JVN#58849431: Multiple vulnerabilities in Cybozu Garoon	Third Party Advisory jvn.jp text/xml	 MISC jvn.jp/en/jp/JVN58849431/index.html

