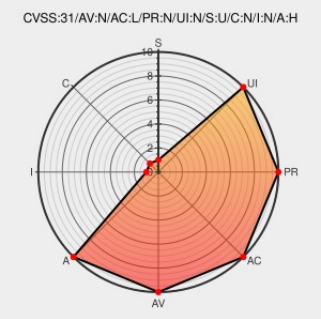
CVE-2020-5622

Published on: 09/02/2020 12:00:00 AM UTC

Last Modified on: 07/12/2022 05:42:00 PM UTC

CVE-2020-5622

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Server Security Type from Shadan-kun contain the following vulnerability:

Shadankun Server Security Type (excluding normal blocking method types) Ver.1.5.3 and earlier allows remote attackers to cause a denial of service which may result in not being able to add newly detected attack source IP addresses as blocking targets for about 10 minutes via a specially crafted request.

CVE-2020-5622 has been assigned by vultures@jpcert.or.jp to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Cyber Security Cloud , Inc.** - **Shadankun Server Security Type (excluding normal blocking method types)** version **Ver.1.5.3 and earlier**

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link

JVN#42665874: "Shadankun Server Security Type" vulnerable to denial-of-service (DoS)	Third Party Advisory jvn.jp text/xml	MISC jvn.jp/en/jp/JVN42665874/index.html
【重要】攻撃遮断くん サーバセキュリティタイプの一部遮断方式におけるDoS（サービス妨害）の脆弱性に関する注意喚起（CVE-2020-5622）｜クラウド型WAF 攻撃遮断くん	Vendor Advisory www.shadan-kun.com text/html	MISC www.shadan-kun.com/news/20200831/

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Shadan-kun	Server Security Type	All	All	All	All

cpe:2.3:a:shadan-kun:server_security_type:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→