

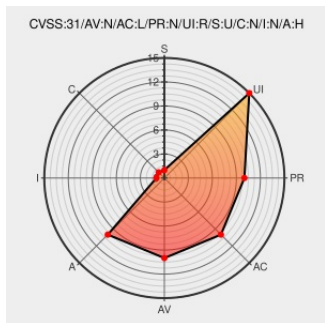


CVE-2020-9343

Published on: 03/19/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-9343

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

Certain versions of [Windows](#) from [Microsoft](#) contain the following vulnerability:

An issue was discovered in signotec signoPAD-API/Web (formerly Websocket Pad Server) before 3.1.1 on Windows. It is possible to perform a Denial of Service attack because the implementation doesn't limit the parsing of nested JSON structures. If a victim visits an attacker-controlled website, this vulnerability can be exploited via WebSocket data with a deeply nested JSON array.

CVE-2020-9343 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
No Description Provided	Exploit Third Party Advisory	MISC www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2019-053.txt

