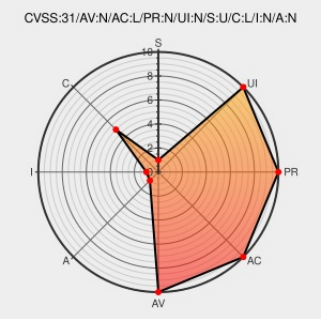
CVE-2019-12163

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

Last Modified on: 03/24/2023 06:27:00 PM UTC

CVE-2019-12163

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



Certain versions of Web Module from Gatship contain the following vulnerability:

GAT-Ship Web Module through 1.30 allows remote attackers to obtain potentially sensitive information via {} in a ws/gatshipWs.asmx/SqlVersion request.

CVE-2019-12163 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.3 - MEDIUM

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Full Disclosure: GAT-Ship Web Module >1.30 - Unauthenticated Information Disclosure Vulnerability	Exploit Mailing List Third Party Advisory seclists.org text/html	MISC seclists.org/fulldisclosure/2019/May/29

Full Disclosure: Re: GAT-Ship Web Module >1.30 - Unauthenticated Information Disclosure Vulnerability	seclists.org text/html	FULLDISC 20190521 Re: GAT-Ship Web Module >1.30 - Unauthenticated Information Disclosure Vulnerability
GAT-Ship Web Module 1.30 Information Disclosure ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/152964/GAT-Ship-Web-Module-1.30-Information-Disclosure.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gatship	Web Module	All	All	All	All

cpe:2.3:a:gatship:web_module:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→