



# CVE-2019-11401

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2019-11401
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-04-22 11:29:00 UTC
<b>Updated</b>	2019-04-24 20:36:00 UTC
<b>Description</b>	A issue was discovered in SiteServer CMS 6.9.0. It allows remote attackers to execute arbitrary code because an administr

## Risk And Classification

**Problem Types:** CWE-434

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Siteserver</a>	<a href="#">Siteserver Cms</a>	6.9.0	All	All	All
Application	<a href="#">Siteserver</a>	<a href="#">Siteserver Cms</a>	6.9.0	All	All	All

## References

Reference	Source
There is a vulnerability that the attacker can uploads a file bypassed the filtering rule to getshell. · Issue #1858 · siteserver/cms · GitHub	MISC
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)