



# CVE-2017-9071

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2017-9071
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-05-18 16:29:00 UTC
<b>Updated</b>	2017-05-30 19:28:00 UTC
<b>Description</b>	In MODX Revolution before 2.5.7, an attacker might be able to trigger XSS by injecting a payload into the HTTP Host header.

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Modx	Modx Revolution	All	All	All	All

## References

Reference	Source
[SECURITY-20] Prevent XSS by cache poisoning via Host header by opengeek · Pull Request #13426 · modxcms/revolution · GitHub	MISC
MODX Revolution CMS 2.5.6 - Multiple Vulnerabilities - CITADELO	MISC
CVE Program record	CVE
NVD vulnerability detail	NVD

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)