



# CVE-2017-8085

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

## Summary

<b>CVE</b>	CVE-2017-8085
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-04-24 14:59:00 UTC
<b>Updated</b>	2017-04-29 01:59:00 UTC
<b>Description</b>	In Exponent CMS before 2.4.1 Patch #5, XSS in eFinder is possible in framework/modules/file/connector/elfinder.php.

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Exponentcms</a>	<a href="#">Exponent Cms</a>	All	p4	All	All

## References

Reference	Source	Link
Release v2.4.1 Patch #5 · exponentcms/exponent-cms · GitHub	CONFIRM	<a href="#">github.com</a>
fix possible xss security issue with eFinder (thanks to chengable) · exponentcms/exponent-cms@0b2241f · GitHub	CONFIRM	<a href="#">github.com</a>
Patch #5 Released for V2.4.1 to fix a few Critical Issues	CONFIRM	<a href="#">www.expo</a>
Exponent CMS CVE-2017-8085 Cross Site Scripting Vulnerability	BID	<a href="#">www.secu</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.o</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.go</a>

No vendor comments have been submitted for this CVE.

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

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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)