



# CVE-2018-0603

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

## Summary

<b>CVE</b>	CVE-2018-0603
<b>State</b>	PUBLIC
<b>Assigner</b>	vultures@jpcert.or.jp
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-06-26 14:29:00 UTC
<b>Updated</b>	2018-08-17 17:12:00 UTC
<b>Description</b>	Cross-site scripting vulnerability in Site Reviews versions prior to 2.15.3 allows remote attackers to inject arbitrary web scrip

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Geminilabs</a>	<a href="#">Site Reviews</a>	All	All	All	All
Application	<a href="#">Geminilabs</a>	<a href="#">Site Reviews</a>	All	All	All	All

## References

Reference	Source	Link	Tags
JVN#60978548: WordPress plugin "Site Reviews" vulnerable to cross-site scripting	JVN	<a href="#">jvn.jp</a>	Third Party Advisory
Site Reviews <= 2.15.2 - Cross-Site Scripting (XSS)	MISC	<a href="#">wpvulndb.com</a>	Third Party Advisory
Site Reviews   WordPress.org	MISC	<a href="#">wordpress.org</a>	Third Party Advisory
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical, analysis

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)