



CVE-2020-14959

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

Summary

CVE	CVE-2020-14959
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-22 00:15:00 UTC
Updated	2020-06-25 20:08:00 UTC
Description	Multiple XSS vulnerabilities in the Easy Testimonials plugin before 3.6 for WordPress allow remote attackers to inject arbitrary HTML and JavaScript via the 'text' parameter in the 'easy_testimonials_shortcode' function.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Goldplugins	Easy Testimonials	All	All	All	All
Application	Goldplugins	Easy Testimonials	All	All	All	All

References

Reference	Source	Link	Tags
Easy Testimonials < 3.6 - Authenticated Stored Cross-Site Scripting (XSS) Security Vulnerability	MISC	wpvulndb.com	Exploit, Third Party
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)