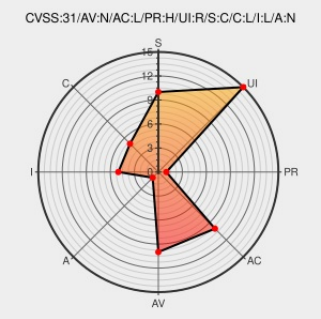
CVE-2022-2473

Published on: Not Yet Published

Last Modified on: 10/24/2023 08:28:00 PM UTC

CVE-2022-2473

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Wp-useronline from Wp-useronline Project contain the following vulnerability:

The WP-UserOnline plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'templates[browsingpage][text]' parameter in versions up to, and including, 2.87.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with administrative capabilities and above to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The only affects multi-site installations and installations where unfiltered_html is disabled.

CVE-2022-2473 has been assigned by security@wordfence.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **gamerz** - **WP-UserOnline** version **<= 2.87.6**

CVSS3 Score: 4.8 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVE References

Description	Tags	Link
Vulnerability Advisories - Wordfence	www.wordfence.com text/html	MISC www.wordfence.com/vulnerability-advisories/#CVE-2022-2473
WordPress Plugin WP-UserOnline 2.87.6 - Stored Cross-Site Scripting (XSS) - PHP webapps Exploit	www.exploit-db.com Proof of Concept text/html	MISC www.exploit-db.com/exploits/50988
WP-UserOnline <= 2.87.6 - Authenticated	www.wordfence.com	MISC www.wordfence.com/threat-

(Admin+) Stored Cross-Site Scripting	text/html	intel/vulnerabilities/id/6a44a55e-a96a-4698-9948-6ef33138a834?source=cve
403 Forbidden	plugins.trac.wordpress.org text/html Inactive Link Not Archived	MISC plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2758412%40wp-useronline&new=2758412%40wp-useronline&sfp_email=&sfph_mail=
WordPress WP-UserOnline 2.87.6 Cross Site Scripting ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/167864/wpuseronline2876-xss.txt
WordPress WP-UserOnline 2.87.6 Cross Site Scripting - Exploitalert	www.exploitalert.com text/html	MISC www.exploitalert.com/view-details.html?id=38912
WordPress Plugin WP-UserOnline 2.87.6 Stored Cross-Site Scripting (XSS) - Exploitalert	www.exploitalert.com text/html	MISC www.exploitalert.com/view-details.html?id=38893
Please update your browser	youtu.be text/html	MISC youtu.be/Q3zInrUnAV0

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wp-useronline Project	Wp-useronline	All	All	All	All

cpe:2.3:a:wp-useronline_project:wp-useronline:*:*:*:*:*:wordpress:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-2473 : The WP-UserOnline plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'templa… twitter.com/i/web/status/1…	2022-09-06 18:08:41
@LinInfoSec	Wordpress - CVE-2022-2473: exploitalert.com/view-details.h…	2022-09-06 21:00:57

← Previous ID

Next ID→

site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report