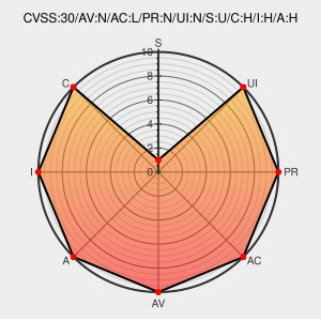
CVE-2019-14230

Published on: 07/21/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:57 PM UTC

CVE-2019-14230

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



Certain versions of Onionbuzz from Onionbuzz contain the following vulnerability:

An issue was discovered in the Viral Quiz Maker - OnionBuzz plugin before 1.2.7 for WordPress. One could exploit the id parameter in the set_count ajax nopriv handler due to there being no sanitization prior to use in a SQL query in saveQuestionVote. This allows an unauthenticated/unprivileged user to perform a SQL injection attack capable of remote code execution and information disclosure.

CVE-2019-14230 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
oss-security - Re: Two unauthenticated SQL injection vulnerabilities in Onionbuzz WordPress plugin	Exploit, Mailing List	MLIST [oss-security] 20190722 Re: Two unauthenticated SQL injection vulnerabilities in Onionbuzz

	Third Party Advisory www.openwall.com text/html	WordPress plugin
oss-security - Two unauthenticated SQL injection vulnerabilities in Onionbuzz WordPress plugin	Exploit Mailing List Third Party Advisory www.openwall.com text/html	MISC www.openwall.com/lists/oss-security/2019/07/21/1

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	Onionbuzz	Onionbuzz	All	All	All	All
Application	Onionbuzz	Onionbuzz	All	All	All	All

cpe:2.3:a:onionbuzz:onionbuzz:*:*:*:*:*:wordpress:*:*:

cpe:2.3:a:onionbuzz:onionbuzz:*:*:*:*:*:wordpress:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→