

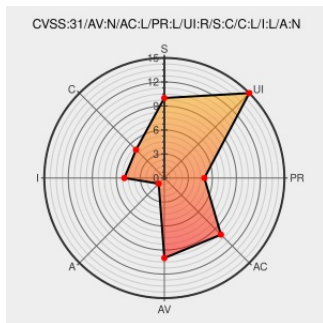


CVE-2021-3258

Published on: 02/05/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:53 PM UTC

CVE-2021-3258

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Q2a Ultimate Seo](#) from [Qa-themes](#) contain the following vulnerability:

Question2Answer Q2A Ultimate SEO Version 1.3 is affected by cross-site scripting (XSS), which may lead to arbitrary remote code execution.

CVE-2021-3258 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.4 - MEDIUM**

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

CVSS2 Score: **3.5 - LOW**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
CVE-2021-3258 S-XSS To Defacement & Acc. Takeover [Q2A Themes] - Nirmal Official	Exploit Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MISC nirmaldahal.com.np/sxss-to-defacement-and-account-takeover/

[Important] Q2A Ultimate SEO: Important Update
- Question2Answer Q&A

[Release Notes](#)
[Vendor Advisory](#)
www.question2answer.org
[text/html](#)

 MISC www.question2answer.org/qa/58520/important-q2a-ultimate-seo-important-update

Sanitizing Meta output · q2a-projects/Q2A-Ultimate-SEO@20069f2 · GitHub

[Patch](#)
[Third Party Advisory](#)
github.com
[text/html](#)

 MISC github.com/q2a-projects/Q2A-Ultimate-SEO/commit/20069f28147c6f2c3acca4e3f6f5154537c5d536

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	Qa-themes	Q2a Ultimate Seo	1.3	All	All	All
Application	Qa-themes	Q2a Ultimate Seo	1.3	All	All	All

cpe:2.3:a:qa-themes:q2a_ultimate_seo:1.3:*:*:*:question2answer:*:*:

cpe:2.3:a:qa-themes:q2a_ultimate_seo:1.3:*:*:*:question2answer:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @elhackernet	Actualizaciones de seguridad muy importantes para #Fortinet - Productos FortiManager & FortiAnalyze - CVE-2021-3258... twitter.com/i/web/status/1...	2021-07-20 17:21:00
 @Pavandep8	medium.com/pentesternepal... #hacker #hacking #security #Pentesting	2021-08-02 04:36:01

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](#).

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