



CVE-2019-8425

Published on: 02/17/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:55 PM UTC

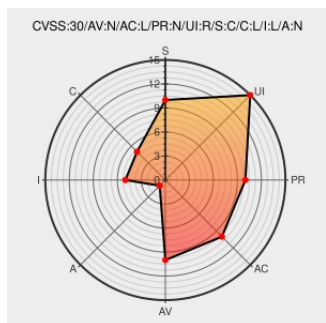
CVE-2019-8425

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Zoneminder](#) from [Zoneminder](#) contain the following vulnerability:

includes/database.php in ZoneMinder before 1.32.3 has XSS in the construction of SQL-ERR messages.

CVE-2019-8425 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
zoneminder反射性xss - 知道创宇 Seebug 漏洞平台	Permissions Required Third Party Advisory www.seebug.org text/html	MISC www.seebug.org/vuldb/ssvid-97764

MISC

github.com/LoRexxar/CVE_Request/tree/master/zoneminder%20vul%20before%20v1.32query-error-reflected-xss

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zoneminder	Zoneminder	All	All	All	All
Application	Zoneminder	Zoneminder	All	All	All	All
cpe:2.3:a:zoneminder:zoneminder:*.*.*.*.*.*.*:						
cpe:2.3:a:zoneminder:zoneminder:*.*.*.*.*.*.*:						

[← Previous ID](#)

Next ID→

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