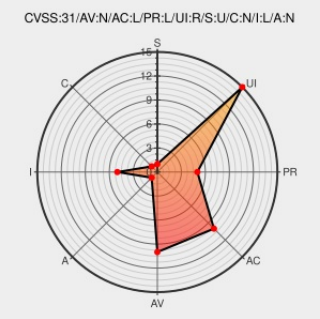
CVE-2017-20056

Published on: Not Yet Published

Last Modified on: 06/28/2022 02:18:00 PM UTC

CVE-2017-20056

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



Certain versions of User Login Log from Intechnosoftware contain the following vulnerability:

A vulnerability was found in weblizar User Login Log Plugin 2.2.1. It has been classified as problematic. Affected is an unknown function. The manipulation leads to basic cross site scripting (Stored). It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.

CVE-2017-20056 has been assigned by cna@vuldb.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **weblizar** - **User Login Log Plugin** version **2.2.1**

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-2017-	vuldb.com	MISC vuldb.com/?id.97386

20056 | weblizar User Login Log Plugin Stored cross site scriting	text/html	
Summer of Pwnage - Stored Cross-Site Scripting vulnerability in User Login Log WordPress Plugin	sumofpwn.nl text/html	MISC sumofpwn.nl/advisory/2016/stored_cross_site_scripting_vulnerability_in_user_login_log_wordpress_plugin.html
Full Disclosure: Stored Cross-Site Scripting vulnerability in User Login Log WordPress Plugin	seclists.org text/html	MISC seclists.org/fulldisclosure/2017/Feb/98

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	Intechnosoftware	User Login Log	2.2.1	All	All	All

cpe:2.3:a:intechnosoftware:user_login_log:2.2.1:*:*:*:*:wordpress:*:*

Discovery Credit

Axel Koolhaas

← Previous ID

Next ID→

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