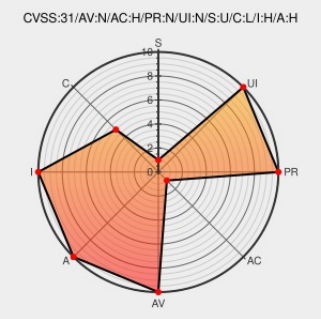
CVE-2022-21647

Published on: 01/04/2022 12:00:00 AM UTC

Last Modified on: 01/20/2022 03:04:00 PM UTC

CVE-2022-21647 - advisory for GHSA-w6jr-wj64-mc9x

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



Certain versions of Codeigniter from Codeigniter contain the following vulnerability:

CodeIgniter is an open source PHP full-stack web framework. Deserialization of Untrusted Data was found in the `old()` function in CodeIgniter4. Remote attackers may inject auto-loadable arbitrary objects with this vulnerability, and possibly execute existing PHP code on the server. We are aware of a working exploit, which can lead to SQL injection. Users are advised to upgrade to v4.1.6 or later. Users unable to upgrade as advised to not use the `old()` function and form_helper nor `RedirectResponse::withInput()` and `redirect()->withInput()`.

CVE-2022-21647 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **codeigniter4** - **CodeIgniter4** version **< 4.1.6**

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
Merge pull request from GHSA-w6jr-wj64-mc9x · codeigniter4/CodeIgniter4@ce95ed5 · GitHub	github.com text/html	MISC github.com/codeigniter4/CodeIgniter4/commit/ce95ed5765256e2f09f3513e7d42790e0d6
Deserialization of Untrusted Data in Codeigniter4 · Advisory · codeigniter4/CodeIgniter4 · GitHub	github.com text/html	CONFIRM github.com/codeigniter4/CodeIgniter4/security/advisories/GHSA-w6jr-wj64

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	Codeigniter	Codeigniter	All	All	All	All

cpe:2.3:a:codeigniter:codeigniter:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-21647 : CodeIgniter is an open source PHP full-stack web framework. Deserialization of Untrusted Data was… twitter.com/i/web/status/1…	2022-01-04 20:10:36
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-21647 Description: CodeIgniter is an open source PHP full-stack web fra… twitter.com/i/web/status/1…	2022-01-04 20:56:12

← Previous ID

Next ID→