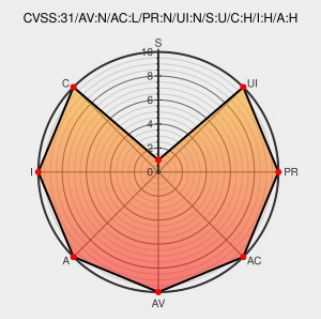
CVE-2022-39365

Published on: Not Yet Published

Last Modified on: 10/31/2022 02:13:00 PM UTC

CVE-2022-39365 - advisory for GHSA-5qxq-vgmm-q39m

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



Certain versions of Pimcore from Pimcore contain the following vulnerability:

Pimcore is an open source data and experience management platform. Prior to version 10.5.9, the user controlled twig templates rendering in `Pimcore/Mail` & `ClassDefinition\Layout\Text` is vulnerable to server-side template injection, which could lead to remote code execution. Version 10.5.9 contains a patch for this issue. As a workaround, one may apply the patch manually.

CVE-2022-39365 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **pimcore** - **pimcore** version **< 10.5.9**

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

CVE References

Description	Tags	Link
[Mail] Renderer email content twig templates in a sandbox by dvesh3 · Pull Request #13347 · pimcore/pimcore · GitHub	github.com text/html	MISC github.com/pimcore/pimcore/pull/13347
RCE vulnerability in Pimcore/Mail & Dynamic Text Layout · Advisory · pimcore/pimcore · GitHub	github.com text/html	CONFIRM github.com/pimcore/pimcore/security/advisories/GHSA-5qxq-vgmm-q39m
Error	github.com	MISC github.com/pimcore/pimcore/pull/13347.patch

	text/x-diff	
[Mail] Renderer email content twig templates in a sandbox (#13347) · pimcore/pimcore@43aa34e · GitHub	github.com text/html	MISC github.com/pimcore/pimcore/commit/43aa34e018f5cd447bceb864358285ba92f68372

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	Pimcore	Pimcore	All	All	All	All

cpe:2.3:a:pimcore:pimcore:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-39365 : Pimcore is an open source data and experience management platform. Prior to version 10.5.9, the us… twitter.com/i/web/status/1…	2022-10-27 14:57:03
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-39365 Pimcore is an open source data and experience management platform… twitter.com/i/web/status/1…	2022-10-27 15:56:02
/r/netcve	CVE-2022-39365	2022-10-27 15:38:42

← Previous ID

Next ID→