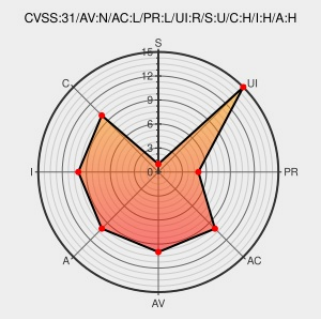
CVE-2022-39369

Published on: Not Yet Published

Last Modified on: 01/11/2023 05:23:00 PM UTC

CVE-2022-39369 - advisory for GHSA-8q72-6qq8-xv64

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



Certain versions of Phpcas from Apereo contain the following vulnerability:

phpCAS is an authentication library that allows PHP applications to easily authenticate users via a Central Authentication Service (CAS) server. The phpCAS library uses HTTP headers to determine the service URL used to validate tickets. This allows an attacker to control the host header and use a valid ticket granted for any authorized service in the same SSO realm (CAS server) to authenticate to the service protected by phpCAS. Depending on the settings of the CAS server service registry in worst case this may be any other service URL (if the allowed URLs are configured to "^(https)://.*") or may be strictly limited to known and authorized services in the same SSO federation if proper URL service validation is applied. This vulnerability may allow an attacker to gain access to a victim's account on a vulnerable CASified service without victim's knowledge, when the victim visits attacker's website while being logged in to the same CAS server. phpCAS 1.6.0 is a major version upgrade that starts enforcing service URL discovery validation, because there is unfortunately no 100% safe default config to use in PHP. Starting this version, it is required to pass in an additional service base URL argument when constructing the client class. For more information, please refer to the upgrading doc. This vulnerability only impacts the CAS client that the phpCAS library protects against. The problematic service URL discovery behavior in phpCAS < 1.6.0 will only be disabled, and thus you are not impacted from it, if the phpCAS configuration has the following setup: 1. `phpCAS::setUrl()` is called (a reminder that you have to pass in the full URL of the current page, rather than your service base URL), and 2. `phpCAS::setCallbackURL()` is called, only when the proxy mode is enabled. 3. If your PHP's HTTP header input `X-Forwarded-Host`, `X-Forwarded-Server`, `Host`, `X-Forwarded-Proto`, `X-Forwarded-Protocol` is sanitized before reaching PHP (by a reverse proxy, for example), you will not be impacted by this vulnerability either. If your CAS server service registry is configured to only allow known and trusted service URLs the severity of the vulnerability is reduced substantially in its severity since an attacker must be in control of another authorized service. Otherwise, you should upgrade the library to get the safe service discovery behavior.

CVE-2022-39369 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **apereo** - **phpCAS** version < **1.6.0**

CVSS3 Score: 8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
Service Hostname Discovery Exploitation · Advisory · apereo/phpCAS · GitHub	github.com text/html	CONFIRM github.com/apereo/phpCAS/security/advisories/GHSA-8q72-6qq8-xv64
[SECURITY] Fedora 36 Update: php-pear-CAS-1.6.0-1.fc36 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2022-37c2d26f59
[SECURITY] Fedora 35 Update: php-pear-CAS-1.6.0-1.fc35 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2022-76b3530ac2
[SECURITY] Fedora 37 Update: php-pear-CAS-1.6.0-1.fc37 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2022-d6c6782130

Related QID Numbers

283305 Fedora Security Update for Hypertext Preprocessor (PHP) (FEDORA-2022-76b3530ac2)

283306 Fedora Security Update for Hypertext Preprocessor (PHP) (FEDORA-2022-37c2d26f59)

283439 Fedora Security Update for Hypertext Preprocessor (PHP) (FEDORA-2022-d6c6782130)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apereo	Phpcas	All	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Operating System	Fedoraproject	Fedora	37	All	All	All

cpe:2.3:a:apereo:phpcas:*:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:35:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:36:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:37:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
/r/netcve	CVE-2022-39369	2022-11-01 16:39:14

← Previous ID

Next ID→