Reset Password / Login vulnerability

Moderate **danrot** published **GHSA-wfm4-pq59-wg6r** on Aug 3, 2020

Package

php **Sulu** (Composer)

Affected versions	Patched versions
<1.6.35, <2.0.10, <2.1.1	1.6.35, 2.0.10, 2.1.1

Description

Impact

What kind of vulnerability is it? Who is impacted?

This vulnerability consists of a few related issues:

Forget password leaks information if the user exists

When the "Forget password" feature on the login screen is used, Sulu asks the user for a username or email address. If the given string is not found, a response with a `400` error code is returned, along with a error message saying that this user name does not exist:

```
{
    "code": 0,
    "message": "Entity with the type \u0022Sulu\\Bundle\\SecurityBundle\\Entity\\User\u0022 and the id \u0022asdf\u0022 not found."
}
```

This enables attackers to retrieve valid usernames.

Forgot password leaks user email if user exists

The response of the "Forgot Password" request returns the email address to which the email was sent, if the operation was successful:

```
{"email":"admin@localhost.local"}
```

This information should not be exposed, as it can be used to gather email addresses.

Response time of login gives hint if the username exists

If the username the user enters in the login screen does not exists, the request responds much faster than if the username exists. This again allows attackers to retrieve valid usernames.

Reset Token for Forgot Password feature is not hashed

The reset token in the user database table is not hashed. That means that somebody could try to request a new password using the Forgot Password feature, and look that up in the database, if the attacker somehow got access to the database. Hashing the reset token would fix that problem.

Patches

This problem was fixed in Release 1.6.34, 2.0.10 and 2.1.1.

Workarounds

Override the files manually in your project and change them accordingly.

Severity

Moderate

CVE ID

CVE-2020-15132

Weaknesses

No CWEs

Credits

Synacktiv-contrib

TomKeur

Prokyonn