# Authentication Bypass via persisted RememberMe cookie

High **nicolas-grekas** published **GHSA-cg23-qf8f-62rr** 3 days ago

| Package | Affected versions | Patched versions |
|---|---|---|
| php **symfony/security-http** (Composer) | >=5.3, <5.4.47 | 5.4.47 |
| | >=6, <6.4.15 | 6.4.15 |
| | >=7, <7.1.8 | 7.1.8 |

## Description

### Description

When consuming a persisted remember-me cookie, Symfony does not check if the username persisted in the database matches the username attached with the cookie, leading to authentication bypass.

### Resolution

The `PersistentRememberMeHandler` class now ensures the submitted username is the cookie owner.

The patch for this issue is available here for branch 5.4.

### Credits

We would like to thank Moritz Rauch - Pentryx AG for reporting the issue and Jérémy Derussé for providing the fix.

**Severity**

High 7.5 / 10

**CVSS v3 base metrics**

| | |
|---|---|
| Attack vector | Network |
| Attack complexity | Low |
| Privileges required | None |
| User interaction | None |
| Scope | Unchanged |
| Confidentiality | High |
| Integrity | None |
| Availability | None |

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

**CVE ID**

CVE-2024-51996

**Weaknesses**

No CWEs

**Credits**

jderusse Remediation developer

m0xr4 Reporter