computer emergency response team
CERT-EU
for the EU institutions, bodies and agencies

CERT-EU Security Advisory 2018-026

Vulnerabilities in PHP

October 16, 2018 — v1.0

History:

- *16/10/2018 — v1.0 – Initial publication*

Summary

On 11th of October 2018, several vulnerabilities have been fixed in PHP, a programming language designed for web applications. According to the Center for Internet Security [1], these vulnerabilities allow an adversary to perform an arbitrary code execution and/or denial-of-service attack (DoS).

Technical Details

The vulnerabilities affect the system in accordance with the associated privileges of the application. The adversary successfully exploiting the vulnerabilities can install programs, view, change or delete data and modify/create users even with admin privileges. A failed exploitation can potentially lead to a state of denial of service [1].

Versions Affected

- PHP 7.2 prior to 7.2.11 [2]
- PHP 7.1 prior to 7.1.23 [3]

Recommendations

1. Check if the system has unauthorized modifications – in case these vulnerabilities have already been exploited.
2. Upgrade to the latest version (either 7.1.23 or 7.2.11)
3. Apply the *Least Privilege* principle to the system and services to limit the impact in case a PHP application is exploited.

References

[1] https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-php-could-allow-for-arbitrary-code-execution_2018-113/

[2] http://php.net/ChangeLog-7.php#7.2.11

[3] http://php.net/ChangeLog-7.php#7.1.23