PHP Vulnerabilities

Tonga National Computer Emergency Response Team

Dear Constituents,

There are multiple vulnerabilities in PHP the most severe of which could allow an attacker to execute arbitrary code. PHP is a programming language originally designed for use in web-based applications with HTML content.
Successfully exploiting the most severe of these vulnerabilities could allow for arbitrary code execution in the context of the affected application. Depending on the privileges associated with the application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploitation could result in a denial-of-service condition.

List of affected versions

- *PHP 7.2 prior to 7.2.10*
- *PHP 7.1 prior to 7.1.22*
- *PHP 7.0 prior to 7.0.32*
- *PHP 5.6 prior to 5.6.38*

What to do

1. Upgrade to the latest version of PHP immediately, after appropriate testing.
2. Verify no unauthorized system modifications have occurred on system before applying patch.
3. Apply the principle of Least Privilege to all systems and services.
4. Remind users not to visit websites or follow links provided by unknown or untrusted sources.

Reference

- https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-php-could-allow-for-arbitrary-code-execution_2018-101/

Please for more information you can contact us:

Tonga National CERTMinistry of MEIDECC
OG Sanft Building Level 2
Nuku'alofa
Tel: 2378 (CERT)
email: report@cert.to
web: www.cert.to

Disclaimer Notice:

The information in this notice is intended solely for public knowledge and awareness, and not intending to harm, fright or disturb any person(s), legal entity or the receiver of this information. Under no circumstances shall the Ministry of MEIDECC be liable for any indirect, incidental, consequential, special or exemplary damages arising out of or in connection with your access or use of or inability to access or use the information and any third party content and services.