Security Advisory 2020-018

Serious PHP Vulnerability

April 03, 2020 — v1.0

TLP:WHITE

History:

• 03/04/2020 — v1.0 – Initial publication

Summary

In PHP versions 7.3.x below 7.3.16 and 7.4.x below 7.4.34, while using `mb_strtolower()` function with UTF-32LE encoding, certain invalid strings could cause PHP to overwrite stack-allocated buffer. This could lead to memory corruption, crashes, and potentially code execution [1]. No exploits have been observed for the moment.

Technical Details

A call to `mb_strtolower()` allows overwriting of a stack-allocated buffer with an overflown array from .rodata (the read-only data segment in memory). It seems that size is well-controlled by an attacker in the range 512-1020, while the data to overwrite with are much less controlled [2].

Products Affected

The vulnerability was coded as CVE-2020-7065 and it affects PHP versions 7.3.0, 7.3.1, 7.3.2, 7.3.3, 7.3.4, 7.3.5, 7.3.6, 7.3.7, 7.3.8, 7.3.9, 7.3.10, 7.3.11, 7.3.12, 7.3.13, 7.3.14, 7.4.0, 7.4.1, 7.4.2 [3]

Recommendations

PHP has released a patch for this vulnerability [4]. It is strongly advised to update to the version 7.4.4 to fix this vulnerability as soon as possible.
References