Security Advisory 2021-068

Fortinet Fortiweb Vulnerability

December 13, 2021 — v1.0

TLP:WHITE

History:

• 13/12/2021 — v1.0 – Initial publication

Summary

On December 7th, Fortinet PSIRT released an advisory to address a heap-based buffer overflow vulnerability in FortiWeb. This vulnerability (CVE-2021-43071) allows an attacker to execute arbitrary code and commands on the affected product [1].

Technical Details

The vulnerability is due to an heap-based buffer overflow in API v1.0 controller. To exploit this vulnerability, an attacker can send crafted HTTP requests to the LogAccess and LogReport API controller to execute arbitrary code or commands.

Affected Products

The affected products are the following:

• FortiWeb version 6.4.1 and below.
• FortiWeb version 6.3.16 and below.
• FortiWeb version 6.2.6 and below.

Recommendations

CERT-EU strongly recommends to upgrade to the following versions:

• FortiWeb version 7.0.0 or above.
• FortiWeb version 6.4.2 or above.
• FortiWeb version 6.3.17 or above.

Fortinet PSIRT also precise that the fix for FortiWeb versions 6.2 has to be confirmed.
References