Security Advisory 2021-061

Critical Vulnerabilities in FortiWeb

November 5, 2021 — v1.0

TLP:WHITE

History:

- *05/11/2021 — v1.0 – Initial publication*

Summary

On November 2, 2021, a critical vulnerability was announced by Fortinet PSIRT. The vulnerability is tracked as CVE-2021-36186 [1, 2]. Very little additional details are available about this vulnerability at this time.

Technical Details

A stack-based buffer overflow vulnerability in FortiWeb may allow an unauthenticated attacker to overwrite the content of the stack and potentially execute arbitrary code by sending crafted HTTP requests with large request parameter values.

Affected Products

This vulnerability affects the following versions:

- FortiWeb version 6.4.0
- FortiWeb versions 6.3.15 and below
- FortiWeb versions 6.2.5 and below

Recommendations

Upgrade to patched versions:

- Upgrade to FortiWeb versions 6.4.1 or above.
- Upgrade to FortiWeb versions 6.3.16 or above.
- Upgrade to FortiWeb versions 6.2.6 or above.

CERT-EU recommends updating the vulnerable application as soon as possible.

Workarounds and Mitigations

There are no known mitigations for this vulnerability.

References

[1] https://www.fortiguard.com/psirt/FG-IR-21-119

[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36186