At a glance:

IR Number	FG-IR-17-137
Date	Nov 03, 2017
Risk	●●●○○
Impact	Man-in-the-Middle (MitM) Attacks
CVE ID	CVE-2009-3555 (http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555)

PSIRT Advisory

FortiOS SSL Deep-Inspection possible Insecure Renegotiation

Summary

FortiOS SSL Deep-Inspection may enable insecure renegotiation between TLS clients and servers that support secure renegotiation, opening the door to potential Man-in-the-Middle attacks (CVE-2009-3555) against the TLS connection, where an attacker could inject arbitrary data in the connection (without however being able to decipher it).

The fix enables secure renegotiation on the SSL Deep-Inspection when both the client and server support it.

Impact

Man-in-the-Middle (MitM) Attacks

Affected Products

FortiOS 5.6.0

FortiOS 5.4.0 to 5.4.5

FortiOS 5.2 and below

Solutions

Upgrade to FortiOS 5.4.6 or 5.6.1

- (https://www.fortinet.com)