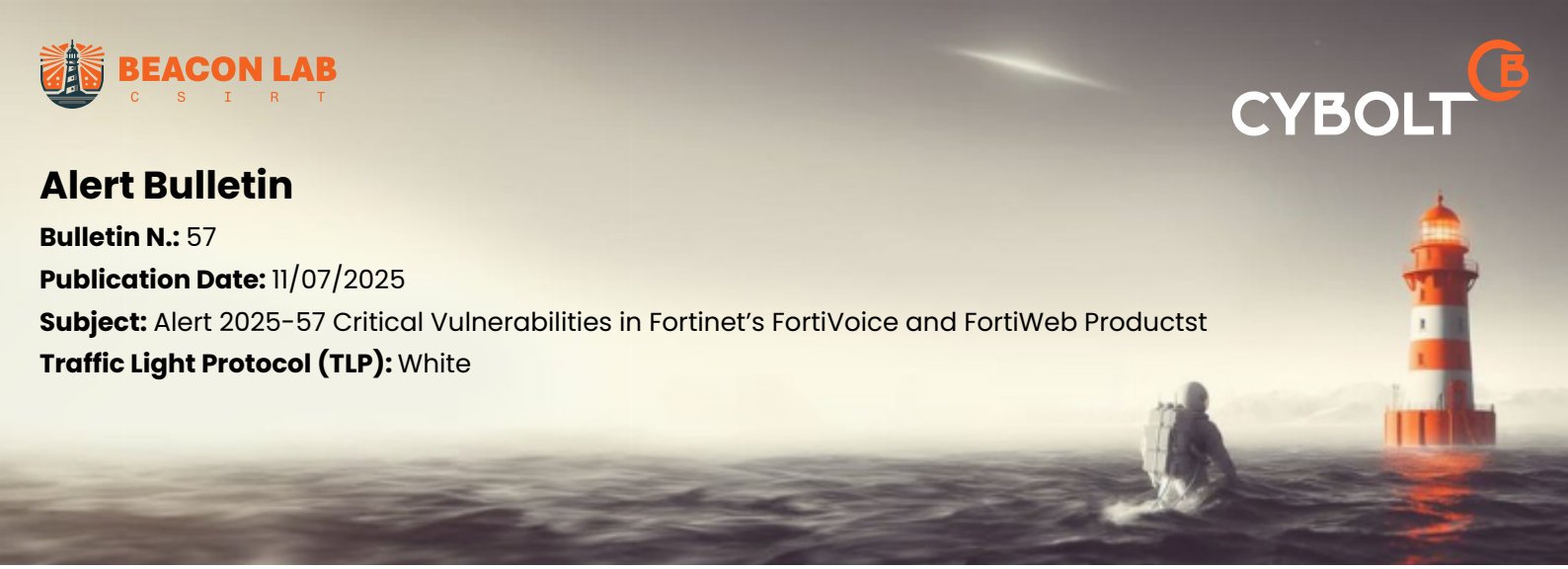

Alert Bulletin

Bulletin N.: 57
Publication Date: 11/07/2025
Subject: Alert 2025-57 Critical Vulnerabilities in Fortinet's FortiVoice and FortiWeb Productst
Traffic Light Protocol (TLP): White

Affected product(s):

- FortiVoice
  - 7.2.07.0.0 to 7.0.6
  - 6.4.0 to 6.4.10
- FortiWeb
  - 7.6.0 to 7.6.37.4.0 to 7.4.77.2.0 to 7.2.10
  - 7.0.0 to 7.0.10
- Among other products

Description

Several important vulnerabilities affecting Fortinet products have been published, including CVE-2025-25257 (CVSS score of 9.6), which affects FortiWeb, and CVE-2025-47856 (CVSS score of 7.2), which affects FortiVoice.

The FortiWeb vulnerability CVE-2025-25257 could be exploited via crafted HTTP or HTTPS requests to execute unauthorized code or SQL commands. Authentication is not required for successful exploitation.

Crafted HTTP/HTTPS or CLI requests could also be used to exploit two high-severity OS command injection flaws in FortiVoice. Identified as CVE-2025-47856 (CVSS score of 7.2), these issues could allow a privileged attacker to execute arbitrary code or commands.

Solution:

It is recommended to apply the security patches recommended by the manufacturer:

FortiWeb

- Branch 7.6: Update to 7.6.4 or higher
- Branch 7.4: Update to 7.4.8 or higher
- Branch 7.2: Update to 7.2.11 or higher

- Branch 7.0: Update to 7.0.11 or higher

FortiVoice

- Branch 7.2: Update to 7.2.1 or higher
- Branch 7.0: Update to 7.0.7 or higher
- Branch 6.4: Update to 6.4.11 or higher

At the following link you can find the Fortinet page to manage your product updates:

https://docs.fortinet.com/upgrade-tool/fortigate

Additional information:

- https://fortiguard.fortinet.com/psirt/FG-IR-25-250
- https://fortiguard.fortinet.com/psirt/FG-IR-25-151
- https://www.securityweek.com/ivanti-fortinet-splunk-release-security-updates