Posted Date: 2025/05/22 \

Vulnerability Alert Fortinet Multiple Products Have Critical Security Vulnerabilities (CVE-2025-32756)

- Subject Description: Vulnerability Alert Fortinet Multiple Products Have Critical Security Vulnerabilities (CVE-2025-32756)
- Content Description:
  - Forwarded by Taiwan Computer Network Crisis Coordination Center TWCERTCC-200-202505-00000016
  - Recently, Fortinet released several products with critical security vulnerabilities (CVE-2025-32756, CVSS: 9.8), affecting FortiVoice, FortiMail, FortiNDR, FortiRecorder, and FortiCamera. This vulnerability is a stack overflow that allows unauthenticated remote attackers to execute arbitrary code or commands via specially crafted HTTP requests.
- Affected Platforms:
  - FortiCamera 2.1.0 to 2.1.3
  - FortiCamera 2.0 all versions
  - FortiCamera 1.1 all versions
  - FortiMail 7.6.0 to 7.6.2
  - FortiMail 7.4.0 to 7.4.4
  - FortiMail 7.2.0 to 7.2.7
  - FortiMail 7.0.0 to 7.0.8
  - FortiNDR 7.6.0
  - FortiNDR 7.4.0 to 7.4.7
  - FortiNDR 7.2.0 to 7.2.4
  - FortiNDR 7.1 all versions
  - FortiNDR 7.0.0 to 7.0.6
  - FortiNDR 1.5 all versions
  - FortiNDR 1.4 all versions
  - FortiNDR 1.3 all versions
  - FortiNDR 1.2 all versions
  - FortiNDR 1.1 all versions
  - FortiRecorder 7.2.0 to 7.2.3
  - FortiRecorder 7.0.0 to 7.0.5
  - FortiRecorder 6.4.0 to 6.4.5
  - FortiVoice 7.2.0
  - FortiVoice 7.0.0 to 7.0.6
  - FortiVoice 6.4.0 to 6.4.10
- Recommended Actions:
  - Please update to the following versions:
  - FortiCamera 2.1.4 and later versions
  - FortiMail 7.6.3 and later versions
  - FortiMail 7.4.5 and later versions
  - FortiMail 7.2.8 and later versions
  - FortiMail 7.0.9 and later versions
  - FortiNDR 7.6.1 and later versions

    - FortiNDR 7.4.8 and later versions
    - FortiNDR 7.2.5 and later versions
    - FortiNDR 7.0.7 and later versions
    - FortiRecorder 7.2.4 and later versions
    - FortiRecorder 7.0.6 and later versions
    - FortiRecorder 6.4.6 and later versions
    - FortiVoice 7.2.1 and later versions
    - FortiVoice 7.0.7 and later versions
    - FortiVoice 6.4.11 and later versions
    - For other unlisted product versions, please migrate to fixed versions
- References:
    - https://www.twcert.org.tw/tw/cp-169-10127-ec862-1.html

Computer and Communication Center \ Network Systems Group