Cisco warned of serious vulnerability in her software secure Firewall Threat Defense (FTD). The error affects the component that is responsible for the analysis of network traffic.

The vulnerability was received by the CVE-2025−20 217 identifier and a high danger rating-8.6 out of 10. It allows remote attackers without authorization to send specially prepared data packages. As a result, the system is focused when checking traffic and stops working, which causes a refusal to maintain (DOS).

Although the built -in recovery mechanism automatically restarts the component, at this moment the system remains without protection, and malicious traffic can go unnoticed. This makes the problem especially dangerous for Cisco devices that work directly on the Internet.

Vulnerability affects only those devices where the SNORT 3 engine is activated and the invasion detection policy is enabled. Cisco Asa, Firewall Management Center (FMC) and earlier version of Snort 2 are not subject to attack.

Cisco emphasizes that it is impossible to circumvent the problem with temporary measures. The only way to protect is to install updates

So far, there are no data on real attacks using this error.