Alert Bulletin

Bulletin N.: 2024-49
Publication Date: 10/10/2024
Subject: Alert 2024-49: Critical Remote Execution Vulnerability in Fortinet Products
Traffic Light Protocol (TLP): White

CISA has issued an alert regarding the active exploitation of a critical remote code execution (RCE) vulnerability in Fortinet products, identified as **CVE-2024-23113**. This vulnerability affects several Fortinet solutions, including FortiOS, FortiPAM, FortiProxy, and FortiWeb.

The flaw is caused by a format string issue in the fgfmd daemon of FortiOS, which could allow an unauthenticated remote attacker to execute arbitrary commands or code on the affected system through crafted requests. The severity of the vulnerability is reflected in its CVSS score of 9.8, classifying it as critical.

According to Shodan data, there are over 15,000 active Fortinet devices in Mexico providing various layers of security in networks and applications.

To mitigate the **CVE-2024-23113** vulnerability in Fortinet products, the solution is to update to the patched versions. Fortinet has released updates that address this vulnerability. For more information, visit the following link: https://support.fortinet.com/