BEACON LAB CSIRT

CYBOLT

Alert Bulletin

Bulletin N.: 2024-12

Publication Date: 31/05/2024

Subject: Alert 2024-12 Publication of Exploit for Fortinet

Traffic Light Protocol (TLP): White

Affected Product(s):

- **FortiClient**
- **FortiSIEM**

Versions:

- **1.0-7.1.1**
- **0.0-7.0.2**
- **7.0-6.7.8**
- **6.0-6.6.3**
- **5.0-6.5.2**
- **4.0-6.4.2**

Description:

On **Tuesday, May 28**, a group of cybersecurity researchers published an exploit for the vulnerability known as **CVE-2024-23109**, which has a critical severity rating and a **CVSS score of 9.8**, affecting **Fortinet FortiSIEM** .

The vulnerability lies in a **SQL command sanitization weakness** that allows command injection at the operating system level as the **root** user. This can be achieved over the network without any third-party interaction.

It is important to note that this vulnerability was disclosed in **February**; however, the publication of the exploit significantly raises the risk of exploitation for users with any of the vulnerable versions of the product. It is strongly recommended to update to a secure version promptly.

Additionally, vulnerabilities in Fortinet products are frequently exploited, leading to ransomware attacks or cyber espionage in corporate or government networks.

Impact:

A malicious actor who can remotely access the **Fortinet FortiSIEM** device can execute the exploit and run commands at the operating system level with privileged user access, potentially leading to catastrophic consequences, as they could take control of the device and extend the attack throughout the network.

Solution:

Apply the official patch published by Fortinet.

Additional Information:

- **Bleeping Computer Article**
- **NVD CVE-2024-23109**