Cyber Security Advisory No. 175 **10-03-2023**

Name: Critical Vulnerability in FortiOS and FortiProxy Could Allow Remote Code Execution

Threat Classification: Remote Code Execution

Affected Version:

- FortiOS version 7.2.0 through 7.2.3
- FortiOS version 7.0.0 through 7.0.9
- FortiOS version 6.4.0 through 6.4.11
- FortiOS version 6.2.0 through 6.2.12
- FortiOS 6.0 all versions
- FortiProxy version 7.2.0 through 7.2.2
- FortiProxy version 7.0.0 through 7.0.8
- FortiProxy version 2.0.0 through 2.0.11
- FortiProxy 1.2 all versions
- FortiProxy 1.1 all versions

Summary:

A critical vulnerability (CVE-2023-25610) has been identified in the administrative interface of FortiOS and FortiProxy, which could enable an unauthenticated attacker to execute arbitrary code on the device and perform a denial-of-service (DoS) attack on the GUI. It is important to note that this vulnerability is not limited to a specific region and affects users globally.

Severity	**Critical**
Attack Vector	**Network**

The vulnerability results from a buffer underflow issue and could be exploited by an attacker to send specially crafted HTTP requests to the targeted device. Successful exploitation of this vulnerability could lead to arbitrary code execution, resulting in a complete compromise of the affected system.

Recommendations:

- Fortinet has released patches for the affected products and recommends users to update their software to the latest available version to mitigate potential risks.

References:

- https://www.fortiguard.com/psirt/FG-IR-23-001