Multiple Vulnerabilities in Fortinet Products

Severity Level: High

Components Affected

- FortiOS version 7.2.5 and 7.4.0 through 7.4.1
- FortiProxy version 7.4.0 through 7.4.1

Overview

Multiple vulnerabilities were identified in Fortinet products. Where an attacker could exploit the vulnerability by sending specially crafted requests to an affected system.

Description

Multiple vulnerabilities have been discovered in various Fortinet products, posing a significant security risk. An improper privilege management vulnerability [CWE-269] in a FortiOS & FortiProxy HA cluster may allow an authenticated attacker to perform elevated actions via crafted HTTP or HTTPS requests and could execute unauthorized code or commands.

Impact

- Remote Code Execution
- Elevation of Privilege

Solution/ Workarounds

Before installation of the software, please visit the software vendor web-site for more details.

Apply fixes issued by the vendor:

- https://docs.fortinet.com/upgrade-tool

Reference

https://www.fortiguard.com/psirt/FG-IR-23-315

Disclaimer

The information provided herein is on an "as is" basis, without warranty of any kind.