Advisory Alert

Alert Number: AAA20211130 **Date:** November 30, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Fortinet	**High**	Privilege Escalation via DLL Hijacking

Description

Affected Product	**Fortinet**
Severity	**High**
Affected Vulnerability	Privilege Escalation via DLL Hijacking (CVE-2021-32592)
Description	Fortinet has released Security Updates addressing Privilege Escalation Vulnerability that exist with multiple Fortinet products. An unsafe search path vulnerability in FortiClient and FortiClient EMS may allow an attacker to use a malicious OpenSSL engine library in the search path to perform a DLL Hijack attack on affected devices.
Affected Products	FortiClient 7.0.0 FortiClient 6.4.6 and below. FortiClient 6.2.x. FortiClient 6.0.x. FortiClient EMS 7.0.0 FortiClient EMS 6.4.6 and below. FortiClient EMS 6.2.x. FortiClient EMS 6.0.x.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-21-088

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.