# Advisory Alert

**Alert Number :** AAA20201029 **Date :** October 29, 2020

**Document Classification Level :** Public Circulation Permitted

**Information Classification Level :** TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| SonicWall | High | Remote code execution |
| Juniper | High | Multiple vulnerabilities |

## Description

| | |
|---|---|
| Affected Product | SonicWall |
| Severity | High |
| Affected Vulnerability | Remote code execution (CVE-2020-5145) |
| Description | SonicWall has released security patch updates addressing a recently found vulnerability which allows a remote attacker to compromise vulnerable system.<br>The flaw exists as the application loads DLL libraries in an insecure manner. In order to exploit this flaw a remote attacker will be using specially crafted .dll file and execute arbitrary code on victim's system. |
| Affected Products | SonicWall Global VPN Client version 4.10.4.0314 and earlier |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2020-0021 |

| | |
|---|---|
| Affected Product | Juniper |
| Severity | High |
| Affected Vulnerability | Multiple vulnerabilities |
| Description | Juniper has released security patch updates addressing multiple vulnerabilities that exists in multiple juniper products. An attacker could use these vulnerabilities to gain access to systems and perform malicious activities. Most of the vulnerabilities are found in the Junos OS. It is highly recommended to apply necessary fixes at earliest to the Juniper products to avoid issues. |
| Affected Products | Multiple products |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://kb.juniper.net/InfoCenter/index?page=content&channel=SECURITY_ADVISORIES |

## 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.**