Advisory Alert

Alert Number: AAA20210531 **Date:** May 31, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Pulse Connect Secure	**High**	Buffer Overflow Vulnerability

Description

Affected Product	Pulse Connect Secure
Severity	**High**
Affected Vulnerability	Buffer Overflow Vulnerability (CVE-2021-22908)
Description	Pulse Secure has released security updates addressing buffer overflow vulnerability that exists in their product. This flaw allows remote authenticated user with privileges to browse SMB shares and execute arbitrary codes as a root user. Pulse secure highly recommends to apply necessary security fixes to avoid issues.
Affected Products	Pulse connect secure 9.0Rx Pulse connect secure 9.1Rx
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44800

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.