



Advisory Alert

Alert Number: AAA20210810

Date: August 10, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Pulse Secure	Critical	Multiple Vulnerabilities

Description

Affected Product	Pulse Secure
Severity	Critical
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-22937, CVE-2021-22933, CVE-2021-22934, CVE-2021-22935, CVE-2021-22936, CVE-2021-22938)
Description	Pulse Secure has released security patch updates addressing multiple vulnerabilities that exists in this product. The most severe could cause privilege escalation, buffer overflow, command injection, cross-site script, remote code execution. Pulse secure strongly encourage you to upgrade to avoid issues.
Affected Products	Prior to update Pulse connect secure 9.1R12
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44858/?kA23Z000000L6oySAC

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.

Financial Sector Computer Security Incident Response Team (FinCSIRT)

LankaClear Pvt Ltd, Level 18, Bank of Ceylon Head Office, BOC Square, 01 Bank of Ceylon Mawatha, Colombo 00100, Sri Lanka

Hotline: + 94 112039777