Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No: 135 **04-05-2021**

Name: Critical Vulnerability in Pulse Connect Secure (CVE-2021-22893)

Threat Classification: Remote code execution

Affected Product: Pulse Connect Secure 9.0R3/9.1R1 and Higher

Summary:

Pulse Connect Secure is vulnerable to an authentication bypass vulnerability exposed by the Windows File Share Browser and Pulse Secure Collaboration features which can allow an unauthenticated user to perform remote arbitrary code execution on the Pulse Connect Secure gateway. This vulnerability has been actively exploited globally.

Severity	**Critical**
Attack Vector	Network
Privileges required	None

For further details, please visit following official link:

- https://nvd.nist.gov/vuln/detail/CVE-2021-22893
- https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44784/

Recommendations:

- Please visit 'Solution' section of the following official link for the remediation of the aforementioned vulnerability:
  - https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44784/
- It is highly recommended to upgrade the Pulse Connect Secure server software version to the **9.1R.11.4**.
- Only use licensed software and avoid download/use of cracked and pirated software.
- Use licensed antivirus and regularly obtain its latest updates with its real-time scanning capabilities enabled.
- In case of any incident, please report to this office.