National Cyber Security Centre

2104201000-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Alert

Pulse Connect Secure RCE Vulnerability (CVE-2021-22893)
2021-04-20

Status: TLP-WHITE

This document is classified using Traffic Light Protocol. Recipients may share TLP-WHITE *information freely, without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.*

Threat Type	Ivanti has released details of a critical vulnerability that was discovered in Pulse Connect Secure (PCS). This authentication by-pass vulnerability can allow an unauthenticated user to perform remote arbitrary file execution on the Pulse Connect Secure gateway. This vulnerability has a critical CVSS score and poses a significant risk to your deployment. Details of actions taken by Pulse Secure can be found here. • **CVE-2021-22893**: Pulse Connect Secure Remote Code Execution Vulnerability (CVSS:3.0 Base Score: 10 - Critical) Ivanti Pulse and their security partners have identified threat groups that are actively exploiting CVE-2021-22893. These attacks also exploit previously patched vulnerabilities in Pulse Secure Connect in addition to the newly disclosed vulnerability. Ivanti have observed threat actors harvesting credentials from various Pulse Secure VPN login flows, which ultimately allowed the actor to use legitimate account credentials to move laterally into the affected environments. In order to maintain persistence to the compromised networks, the actor utilized legitimate, but modified, Pulse Secure binaries and scripts on the VPN appliance. The threat actors were able to bypass multifactor authentication requirements, inject webshells, modify files and remove evidence of their activity.
Products Affected	PCS 9.0R3 and Higher
Impact	Remote Code Execution - compromised systems, data loss.
Recommendations	The NCSC recommends that affected organisations review the guidance and advice provided by Pulse and to monitor updates about the issue. Pulse advises that organisations update their Pulse Secure Connect to 9.1R.11.4 immediately in order to prevent exploitation of previously patched vulnerabilities. Ivanti are currently developing a patch for the newly discovered CVE-2021-22893 and this is expected to be delivered in May 2021. Details of this process are on the advisory notice published by Pulse. Ivanti have developed a tool for customers to evaluate their Pulse Connect Secure installations and evaluate any impact from the issues. The Ivanti Pulse Security Integrity Checker Tool is available here. Some frequently asked questions about the tool are answered at this page. Fireeye provide additional information about the threat actors activity and current attribution on their blog and have released signature rules for Snort and Yara. This incident is the latest in a recent trend of attacks against network devices. It highlights the importance of adopting a robust update policy for these devices. The NCSC advises that administrators review their device patching policy in light of the increased activity against network devices, to ensure that vendor-authorised patches are applied efficiently.

DISCLAIMER: *This document is provided "as is" without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.*

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie