NCSC
National Cyber Security Centre

2105041000-NCSC

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

NCSC Alert

Pulse Connect Secure Buffer Overflow Vulnerability (CVE-2021-22908)
2021-05-18

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 vulnerability that was discovered in Pulse Connect Secure (PCS). This includes buffer overflow vulnerability on the Pulse Connect Secure gateway that allows a remote authenticated user with privileges to browse SMB shares to execute arbitrary code as the root user. This vulnerability has a high CVSS score and poses a risk to your deployment. Ivanti have released a workaround to mitigate the risk until a patch is released. • **CVE-2021-22908**: Pulse Connect Secure Buffer Overflow Vulnerability (CVSS:3.11 Base Score: 8.5- High) Ivanti Pulse and their security partners have identified threat groups that are actively exploiting previously patched vulnerabilities in Pulse Secure Connect. This criminal activity increases risk to constituents that do not implement the workaround and patch their Pulse devices. .
Products Affected	PCS 9.0R3 and 9.1RX
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 apply the workaround described in that document. Please note that when the patch is applied, the workaround should be reversed. Details to complete this are also in the document. 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 advise 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