National Cyber Security Centre

2404050146-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Multiple Vulnerabilities Disclosed in Ivanti Products

Friday 5th April, 2024

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared 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.

Description

Vulnerabilities have been discovered in Ivanti Connect Secure (ICS), (formerly known as Pulse Connect Secure) and Ivanti Policy Secure gateways and a patch is available now. **CVE-2024-21894**, **CVE-2024-22052**, **CVE-2024-22053** and **CVE-2024-22023** could allow an attacker to cause remote arbitrary code execution, remote denial of service and breach of data confidentiality.

Products Affected

All supported versions of Ivanti Connect Secure (ICS) and Ivanti Policy Secure gateways – **Version 9.x and 22.x**.

Impact

- **CVE-2024-21894** (Heap overflow vulnerability - **CVSS 8.2**) in IPSec component could allow an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack. In certain conditions this may lead to execution of arbitrary code.
- **CVE-2024-22052** (Null pointer dereference vulnerability - **CVSS 7.5**) in IPSec component could allow an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack.
- **CVE-2024-22053** (Heap overflow vulnerability - **CVSS 8.2**) in IPSec component could allow an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack or in certain conditions read contents from memory.
- **CVE-2024-22023** (XML entity expansion or XEE vulnerability - **CVSS 5.3**) in SAML component could allow an unauthenticated attacker to send specially crafted XML requests in-order-to temporarily cause resource exhaustion thereby resulting in a limited-time DoS.

To date, there have been no reports of the active exploitation of these vulnerabilities.

Recommendations

The NCSC strongly advises affected organisations to identify and update affected Ivanti systems to the latest version.

Further information can be found here:

- Ivanti Security Advisory

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@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie