National Cyber Security Centre

2403200176-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Multiple Vulnerabilities Discovered Within Ivanti Products

Thursday 21st March, 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

Ivanti, in partnership with third-party researchers, have discovered two critical vulnerabilities - **CVE-2023-46808** which affects Ivanti Neurons for ITSM and has a CVSS score of 9.9 and **CVE-2023-41724** which affects Ivanti Standalone Sentry and has a CVSS score of 9.6.

Patches are available for all supported versions of the affected products.

Products Affected

- CVE-2023-46808: Ivanti Neurons for ITSM.
- CVE-2023-41724: Ivanti Standalone Sentry.

Impact

- Exploitation of CVE-2023-46808 could enable an authenticated remote user to perform file writes to the ITSM server.
- Exploitation of CVE-2023-41724 could allow an unauthenticated attacker to execute arbitrary commands on the underlying operating system of the appliance within the same physical or logical network.

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

Recommendations

The NCSC strongly advises affected organisations identify and update affected Ivanti on-premise systems to the latest version. Patches have already been applied to those residing in the Ivanti cloud.

Ivanti advisories for each of the vulnerabilities can be found at the below links:

- https://www.ivanti.com/blog/security-update-for-ivanti-neurons-for-itsm
- https://www.ivanti.com/blog/security-update-for-ivanti-standalone-sentry

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