National Cyber Security Centre

2302280110-NCSC

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

NCSC Alert

Exploitation affecting IBM's Aspera Faspex using CVE-2022-47986

Wednesday 1st March, 2023

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

Threat Actors have been observed actively exploiting a recently identified, high severity vulnerability in IBM's Aspera Faspex file transfer solution. The vulnerability is tracked as CVE-2022-47986 and classified as 'high severity' with a CVSS score of 9.8.

By sending a specially-crafted obsolete API call, a remote attacker could exploit this vulnerability to execute arbitrary code on a vulnerable system. The obsolete API call was removed in Faspex 4.4.2 PL2 (Patch Level 2).

You can view IBM's security bulletin here, which also addresses a number of other vulnerabilities:

https://www.ibm.com/support/pages/node/6952319.

Products Affected

The following versions of IBM's Aspera Faspex are vulnerable to CVE-2022-47986:

- IBM Aspera Faspex 4.4.2 Patch Level 1 and earlier

Impact

Exploitation of CVE-2022-47986 could allow an unauthorised remote attacker to execute arbitrary code on the system which could lead to compromised systems, denial of service, reputational damage and/or data loss.

There have been recent reports of active exploitation of this vulnerability in the wild.

Recommendations

The NCSC strongly advises affected organisations to identify any assets that are running IBM Aspera Faspex 4.4.2 Patch Level 1 and earlier and to upgrade to IBM Aspera Faspex 4.4.2 PL2.

Further information from IBM on this fix for Windows and Linux platforms can be found here:

- Windows
- Linux

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
LinkedIn: ncsc-ie