

CVE-2022-47986

IBM Aspera Faspex Code Execution Vulnerability

Exigent

CISA KEV since Feb 21, 2023

Actively exploited

Ransomware use known

IBM Aspera Faspex 4.4.2 Patch Level 1 and earlier could allow a remote attacker to execute arbitrary code on the system, caused by a YAML deserialization flaw. By sending a specially crafted obsolete API call, an attacker could exploit this vulnerability to execute arbitrary code on the system. The obsolete API call was removed in Faspex 4.4.2 PL2. IBM X-Force ID: 243512.

EVRS 94/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.999 99.98th percentile · FIRST	CISA DEADLINE Mar 14, 2023 KEV since 2023 · listed over a year
--	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☒ Ransomware	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.999 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
aspera faspex	≤ 4.4.1 4.4.2	after 4.4.1	NVD
linux kernel	—	no fixed version listed	NVD
windows	—	no fixed version listed	NVD

Sources

Vendor guidance	ibm.com/support/pages/node/6952319	Additional guidance	exchange.xforce.ibmcloud.com/vulnerabilities/243512
exchange.xforce.ibmcloud.com	exchange.xforce.ibmcloud.com/vulnerabilities/243512?_ga=2.189195179.1800390251.1676559338-700333034.1676325890	NVD	nvd.nist.gov/vuln/detail/CVE-2022-47986
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2022-50700
Current data	evulnable.com/vulnerability-management/cve/CVE-2022-47986		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.