

CVE-2013-3993

IBM InfoSphere BigInsights Invalid Input Vulnerability

CISA KEV since May 25, 2022

Actively exploited

Ransomware use known

IBM InfoSphere BigInsights before 2.1.0.3 allows remote authenticated users to bypass intended file and directory restrictions, or access untrusted data or code, via crafted parameters in unspecified API calls.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 6.5 Medium · NVD	EPSS 0.048 91.9th percentile · FIRST	CISA DEADLINE Jun 15, 2022 KEV since 2022 · 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	0.048 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 6.5	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle No patch reported by the connected remediation source**CISA required action:** The impacted product is end-of-life and should be disconnected if still in use.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
infosphere biginsights	< 2.1.0.3	2.1.0.3	NVD

Sources

Vendor guidance	exchange.xforce.ibmcloud.com/vulnerabilities/84982	NVD	nvd.nist.gov/vuln/detail/CVE-2013-3993
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2013-3925
Current data	evulnable.com/vulnerability-management/cve/CVE-2013-3993		

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