

CVE-2022-29464

WSO2 Multiple Products Unrestrictive Upload of File Vulnerability

Exigent

CISA KEV since Apr 25, 2022

Actively exploited

Ransomware use known

Public exploit module (Metasploit)

Certain WSO2 products allow unrestricted file upload with resultant remote code execution. The attacker must use a /fileupload endpoint with a Content-Disposition directory traversal sequence to reach a directory under the web root, such as a ../../../../repository/deployment/server/webapps directory. This affects WSO2 API Manager 2.2.0 up to 4.0.0, WSO2 Identity Server 5.2.0 up to 5.11.0, WSO2 Identity Server Analytics 5.4.0, 5.4.1, 5.5.0 and 5.6.0, WSO2 Identity Server as Key Manager 5.3.0 up to 5.11.0, WSO2

EVRs

94/100

Immediate priority

CVSS V3.1

9.8

Critical · NVD

EPSS

0.999

99.99th percentile · FIRST

CISA DEADLINE

May 16, 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	0.999 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

Enterprise Integrator 6.2.0 up to 6.6.0, WSO2 Open Banking AM 1.4.0 up to 2.0.0 and WSO2 Open Banking KM 1.4.0, up to 2.0.0.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
api manager	≥ 2.2.0 ≤ 4.0.0	after 4.0.0	NVD
enterprise integrator	≥ 6.2.0 ≤ 6.6.0	after 6.6.0	NVD
identity server	≥ 5.2.0 ≤ 5.11.0	after 5.11.0	NVD
identity server analytics	5.4.0 5.4.1 5.5.0 5.6.0	no fixed version listed	NVD
identity server as key manager	≥ 5.3.0 ≤ 5.10.0	after 5.10.0	NVD
open banking am	≥ 1.3.0 ≤ 2.0.0	after 2.0.0	NVD
open banking iam	2.0.0	no fixed version listed	NVD
open banking km	≥ 1.3.0 ≤ 1.5.0	after 1.5.0	NVD



Sources

Vendor guidance github.com/advisories/GHSA-mfgw-52pj-hrhg

Additional guidance security.docs.wso2.com/en/latest/security-announcements/security-advisories/2022/WS02-2021-1738/

NVD nvd.nist.gov/vuln/detail/CVE-2022-29464

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2022-33802

Current data evulnable.com/vulnerability-management/cve/CVE-2022-29464

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