



# WSO2 Multiple Products Unrestrictive Upload of File Vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2022-29464
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-04-18 22:15:00 UTC
<b>Updated</b>	2023-10-23 22:15:00 UTC
<b>Description</b>	Certain WSO2 products allow unrestricted file upload with resultant remote code execution. The attacker must use a /fileup

## Risk And Classification

**EPSS:** 0.944340000 probability, percentile 0.999860000 (date 2026-05-12)

**CISA KEV:** Listed on 2022-04-25; due 2022-05-16; ransomware use Known

**Problem Types:** CWE-22

## CISA Known Exploited Vulnerability

<b>Vendor</b>	WSO2
<b>Product</b>	Multiple Products
<b>Name</b>	WSO2 Multiple Products Unrestrictive Upload of File Vulnerability
<b>Required Action</b>	Apply updates per vendor instructions.
<b>Notes</b>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2022-29464">https://nvd.nist.gov/vuln/detail/CVE-2022-29464</a>

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Wso2</a>	<a href="#">Api Manager</a>	All	All	All	All
Application	<a href="#">Wso2</a>	<a href="#">Enterprise Integrator</a>	All	All	All	All
Application	<a href="#">Wso2</a>	<a href="#">Identity Server</a>	All	All	All	All
Application	<a href="#">Wso2</a>	<a href="#">Identity Server Analytics</a>	5.4.0	All	All	All
Application	<a href="#">Wso2</a>	<a href="#">Identity Server Analytics</a>	5.4.1	All	All	All
Application	<a href="#">Wso2</a>	<a href="#">Identity Server Analytics</a>	5.5.0	All	All	All
Application	<a href="#">Wso2</a>	<a href="#">Identity Server Analytics</a>	5.6.0	All	All	All

Application	Wso2	Identity Server As Key Manager	All	All	All	All
-------------	------	--------------------------------	-----	-----	-----	-----

## References

Reference	Source	Link
oss-security - CVE-2022-29464 :: WSO2 Unrestricted arbitrary file upload, and remote code to execution vulnerability.	MLIST	<a href="http://www.oss-security.com">www.oss-security.com</a>
GitHub - hakivvi/CVE-2022-29464: WSO2 RCE (CVE-2022-29464) exploit and writeup.	MISC	<a href="https://github.com/hakivvi/CVE-2022-29464">github.com</a>
Security Advisory WSO2-2021-1738 - WSO2 Platform Security - WSO2 Documentation	MISC	<a href="https://docs.wso2.com">docs.wso2.com</a>
Just a moment...	MISC	<a href="https://security.wso2.com">security.wso2.com</a>
WSO Arbitrary File Upload / Remote Code Execution ≈ Packet Storm	MISC	<a href="https://packetstormsecurity.com">packetstormsecurity.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>
CISA Known Exploited Vulnerabilities catalog	CISA	<a href="https://www.cisa.gov">www.cisa.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">150524</a> WSO2 File Upload Remote Command Execution Vulnerability (CVE-2022-29464)
<a href="#">150581</a> WSO2 File Upload Remote Command Execution Vulnerability (CVE-2022-29464)
<a href="#">730453</a> WSO2 Remote Code Execution (RCE) Vulnerability (CVE-2022-29464)
<a href="#">730454</a> WSO2 API Manager Unrestricted Arbitrary File Upload and Remote Code Execution (RCE) Vulnerability (WSO2-2021-1738)
<a href="#">730457</a> WSO2 Unrestricted Arbitrary File Upload and Remote Code Execution (RCE) Vulnerability (WSO2-2021-1738) (Intrusive Check)

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.cve.org). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses/mitre).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)