



Microsoft Exchange Server Remote Code Execution Vulnerability

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

Summary

CVE	CVE-2023-21529
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-02-14 20:15:11 UTC
Updated	2026-04-14 14:44:35 UTC
Description	Microsoft Exchange Server Remote Code Execution Vulnerability

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from secure@microsoft.com

CVSS: 3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.350170000 probability, percentile 0.970380000 (date 2026-04-18)

CISA KEV: Listed on 2026-04-13; due 2026-04-27; ransomware use Unknown

Problem Types: CWE-502 | CWE-502 CWE-502: Deserialization of Untrusted Data

Version	Source	Type	Score	Severity	Vector
3.1	secure@microsoft.com	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CISA Known Exploited Vulnerability

Vendor	Microsoft
Product	Exchange Server
Name	Microsoft Exchange Server Deserialization of Untrusted Data Vulnerability
Required Action	Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.
Notes	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21529 ; https://nvd.nist.gov/vuln/detail/CVE-2023-21529

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Exchange Server	2013	cumulative_update_23	All	All
Application	Microsoft	Exchange Server	2016	cumulative_update_23	All	All
Application	Microsoft	Exchange Server	2019	cumulative_update_11	All	All
Application	Microsoft	Exchange Server	2019	cumulative_update_12	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Microsoft	Microsoft Exchange Server 2019 Cumulative Update 12	affected 15.02.0 15.02.1118.025 custom	x64-based System
CNA	Microsoft	Microsoft Exchange Server 2019 Cumulative Update 11	affected 15.02.0 15.02.0986.041 custom	x64-based System
CNA	Microsoft	Microsoft Exchange Server 2013 Cumulative Update 23	affected 15.00.0 15.00.1497.047 custom	x64-based System
CNA	Microsoft	Microsoft Exchange Server 2016 Cumulative Update 23	affected 15.01.0 15.01.2507.021 custom	x64-based System

References

Reference	Source	Link
Security Update Guide - Microsoft Security Response Center	af854a3a-2127-422b-91ae-364da2661108	msrc.m
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3-4a467353bcc0	www.ci
www.microsoft.com/en-us/security/blog/2026/04/06/storm-1175-focuses-gaze-on-vul...	134c704f-9b21-4f2e-91b3-4a467353bcc0	www.m
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist
CISA Known Exploited Vulnerabilities catalog	CISA	www.ci

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2026-04-13T00:00:00.000Z	CVE-2023-21529 added to CISA KEV

Legacy QID Mappings

- [50125](#) Microsoft Exchange Server Remote Code Execution (RCE) Vulnerability for February 2023
- [730805](#) Microsoft Exchange Server Remote Code Execution (RCE) Vulnerability for February 2023 (Unauthenticated 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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

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

CVE.report and Source URL Uptime Status [status.cve.report](#)