



# Microsoft Purview eDiscovery Elevation of Privilege Vulnerability

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

## Summary

|                 |                                                                                                                               |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2026-26150                                                                                                                |
| State           | PUBLISHED                                                                                                                     |
| Assigner        | microsoft                                                                                                                     |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                  |
| Published       | 2026-04-23 22:16:23 UTC                                                                                                       |
| Updated         | 2026-04-29 19:10:35 UTC                                                                                                       |
| Description     | Server-side request forgery (ssrf) in Microsoft Purview allows an unauthorized attacker to elevate privileges over a network. |

## Risk And Classification

**Primary CVSS:** v3.1 10 CRITICAL from nvd@nist.gov

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

**EPSS:** 0.000900000 probability, percentile 0.251580000 (date 2026-05-05)

**Problem Types:** CWE-918 | CWE-918 CWE-918: Server-Side Request Forgery (SSRF)

| Version | Source               | Type      | Score | Severity | Vector                                                     |
|---------|----------------------|-----------|-------|----------|------------------------------------------------------------|
| 3.1     | nvd@nist.gov         | Primary   | 10    | CRITICAL | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H               |
| 3.1     | secure@microsoft.com | Secondary | 8.6   | HIGH     | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N               |
| 3.1     | CNA                  | CVSS      | 8.6   | HIGH     | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N/E:U/RL:O/RC:C |

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

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



NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor    | Product            | Version | Update | Edition | Language |
|-------------|-----------|--------------------|---------|--------|---------|----------|
| Application | Microsoft | Purview Ediscovery | -       | All    | All     | All      |

Vendor Declared Affected Products

| Source | Vendor    | Product                      | Version    | Platforms     |
|--------|-----------|------------------------------|------------|---------------|
| CNA    | Microsoft | Microsoft Purview EDiscovery | affected - | Not specified |

References

| Reference                                                    | Source               | Link               | Tags                |
|--------------------------------------------------------------|----------------------|--------------------|---------------------|
| msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26150 | secure@microsoft.com | msrc.microsoft.com | Vendor Advisory     |
| CVE Program record                                           | CVE.ORG              | www.cve.org        | canonical           |
| NVD vulnerability detail                                     | NVD                  | nvd.nist.gov       | canonical, analysis |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© 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