



# NuGet Gallery: Arbitrary Blob Overwrite via Nuspec Confusion and URI Fragment Truncation

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

## Summary

<b>CVE</b>	CVE-2026-39399
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-14 23:16:29 UTC
<b>Updated</b>	2026-04-17 15:38:09 UTC
<b>Description</b>	NuGet Gallery is a package repository that powers nuget.org. A security vulnerability exists in the NuGetGallery backend jo

## Risk And Classification

**Primary CVSS:** v3.1 9.6 CRITICAL from security-advisories@github.com

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

**EPSS:** 0.002640000 probability, percentile 0.499470000 (date 2026-04-17)

**Problem Types:** CWE-20 | CWE-22 | CWE-20 CWE-20: Improper Input Validation | CWE-22 CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	9.6	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:H
3.1	CNA	DECLARED	9.6	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

None

Integrity

High

Availability

High

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	NuGet	NuGetGallery	affected < 0e80f87628349207cdcaf55358491f8a6f1ca276	Not specified

### References

Reference	Source	Link	Tags
github.com/NuGet/NuGetGallery/commit/0e80f87628349207cdcaf55358491f8a6f1...	security-advisories@github.com	github.com	
github.com/NuGet/NuGetGallery/security/advisories/GHSA-9r3h-v4hx-rhfr	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	cancel
NVD vulnerability detail	NVD	nvd.nist.gov	cancel

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](https://cve.report/api)

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