



# Vulnerability in Notepad++

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

## Summary

<b>CVE</b>	CVE-2026-3008
<b>State</b>	PUBLISHED
<b>Assigner</b>	CSA
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-27 07:16:03 UTC
<b>Updated</b>	2026-04-27 14:16:47 UTC
<b>Description</b>	Successful exploitation of the string injection vulnerability could allow an attacker to obtain memory address information or c

## Risk And Classification

**Primary CVSS:** v3.1 6.6 MEDIUM from 5f57b9bf-260d-4433-bf07-b6a79e9bb7d4

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

**Problem Types:** CWE-134 | CWE-134 CWE-134 Use of Externally-Controlled Format String

Version	Source	Type	Score	Severity	Vector
3.1	5f57b9bf-260d-4433-bf07-b6a79e9bb7d4	Secondary	6.6	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:H
3.1	CNA	CVSS	6.6	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:H

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

High

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Notepad</a>	<a href="#">Notepad</a>	affected 8.9.3	Not specified

### References

Reference	Source	Link
<a href="https://community.notepad-plus-plus.org/topic/27500/notepad-v8-9-4-release-candidate">community.notepad-plus-plus.org/topic/27500/notepad-v8-9-4-release-candidate</a>	5f57b9bf-260d-4433-bf07-b6a79e9bb7d4	<a href="https://community.notepad-plus-plus.org/topic/27500/notepad-v8-9-4-release-candidate">community.notepad-plus-plus.org/topic/27500/notepad-v8-9-4-release-candidate</a>
<a href="https://lgsjism.github.io/cve-2026-3008">lgsjism.github.io/cve-2026-3008</a>	5f57b9bf-260d-4433-bf07-b6a79e9bb7d4	<a href="https://lgsjism.github.io/cve-2026-3008">lgsjism.github.io/cve-2026-3008</a>
<a href="https://github.com/notepad-plus-plus/notepad-plus-plus/issues/17960">github.com/notepad-plus-plus/notepad-plus-plus/issues/17960</a>	5f57b9bf-260d-4433-bf07-b6a79e9bb7d4	<a href="https://github.com/notepad-plus-plus/notepad-plus-plus/issues/17960">github.com</a>
<a href="https://github.com/lgsjism/cve-2026-3008">github.com/lgsjism/cve-2026-3008</a>	134c704f-9b21-4f2e-91b3-4a467353bcc0	<a href="https://github.com/lgsjism/cve-2026-3008">github.com</a>
<a href="https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2026-044">www.csa.gov.sg/alerts-and-advisories/alerts/al-2026-044</a>	5f57b9bf-260d-4433-bf07-b6a79e9bb7d4	<a href="https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2026-044">www.csa.gov.sg</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>

No vendor comments have been submitted for this CVE.

### Additional Advisory Data

#### Solutions

**CNA:** Users and administrators of the affected product version are advised to update to the latest version 8.9.4 immediately.

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)