

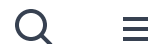


 A Singapore Government Agency Website [How to identify](#) 

 Government officials will never ask you to transfer money or disclose bank log-in details over a phone call. 

Call the 24/7 ScamShield Helpline at 1799 if you are unsure if something is a scam.



[Home](#) > [Alerts & Advisories](#) > [Alerts](#) > [Vulnerability in Notepad++](#)

Alerts

Vulnerability in Notepad++

27 April 2026

CSA has issued a CVE ID to a vulnerability reported in Notepad++ as part of CSA's Responsibility Vulnerability Disclosure Policy. Users and administrators of the affected product version are advised to update to the latest version 8.9.4 immediately.

Background

CSA has issued a CVE ID (CVE-2026-3008) to a vulnerability reported in Notepad++, an open-source text editor. The Product Owner of Notepad++ has released a security update to address the vulnerability.

Impact

Successful exploitation of the string injection vulnerability could allow an attacker to obtain memory address information or crash the application.

Affected Products

The vulnerability affects Notepad++ version 8.9.3.

Mitigation

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

Special Thanks to:

- Informer: Mr Hazley Samsudin
- Product Owner: Notepad++

References

<https://community.notepad-plus-plus.org/topic/27500/notepad-v8-9-4-release-candidate>

[↗](#)

<https://github.com/llgsjms/cve-2026-3008> [↗](#)

<https://llgsjms.github.io/cve-2026-3008/> [↗](#)

<https://github.com/notepad-plus-plus/notepad-plus-plus/issues/17960> [↗](#)

[↑ Back to top](#)

Cyber Security Agency of Singapore

About CSA

Information for

Alerts & Advisories

News & Events

Legislation

Our Programmes

Resources

Careers

[Internet Hygiene Portal](#)

Reach us



Contact

[Feedback](#)

© 2026 Government of Singapore, last updated 27 April 2026

[Report Vulnerability](#)

[Privacy Statement](#)

[Terms of Use](#)

[REACH](#)

Made with



Built by

