

Search

Security Alert: CVE-2026-2123 A high severity privilege escalation vulnerability has been discovered in OpenText™ Operations Agent.

A security audit identified a privilege escalation vulnerability in Operations Agent on Windows. Under specific conditions Operations Agent may run executables from specific writeable locations. CVE-2026-2123

Mar 31, 2026 Knowledge

URL Name

KM000046068

Products

Operations Agent (OA)

Article Body

Summary

A high severity privilege escalation vulnerability has been discovered in OpenText™ Operations Agent 12.29 and earlier on Windows OS.

Systems affected: Operations Agent 12.29 and earlier on Windows OS.

Details:

A security audit identified a privilege escalation vulnerability in Operations Agent on Windows. Under specific conditions Operations Agent may run executables from specific writeable locations.

CVE: reference: CVE-2026-2123

Impact: A low-privileged user could potentially cause code execution with SYSTEM-level privileges on the local system. The issue requires local system access for the attacker.

RESOLUTION

A hotfix has been created which will enforce explicit, fully qualified paths when launching executables.

- The hotfix can be downloaded from the [Marketplace \(https://marketplace.opentext.com/itom/content/operations-agent-hotfix-for-cve-2026-2123-privilege-escalation/\)](https://marketplace.opentext.com/itom/content/operations-agent-hotfix-for-cve-2026-2123-privilege-escalation/) for the OA versions mentioned below.
<https://marketplace.opentext.com/itom/content/operations-agent-hotfix-for-cve-2026-2123-privilege-escalation>
<https://marketplace.opentext.com/itom/content/operations-agent-hotfix-for-cve-2026-2123-privilege-escalation>
- Please follow the readme.txt included in the hotfix zip file for install instructions.

OA 12.24 - HFWIN_1224028.tar, HFWIN_1224029.tar

OA 12.25 - HFWIN_1225045.tar, HFWIN_1225046.tar

OA 12.26 - HFWIN_1226039.tar, HFWIN_1226040.tar

OA 12.27 - HFWIN_1227023.tar, HFWIN_1227024.tar

OA 12.28 - HFWIN_1228020.tar, HFWIN_1228021.tar

OA 12.29 - HFWIN_1229006.tar, HFWIN_1229007.tar

Document Type

Security Bulletins

Article Total View Count

547

Article Created Date

3/24/2026 6:54 PM

Last Published Date

3/31/2026 4:09 PM

Cookies Preferences

We use cookies and similar technologies (including third party cookies from our partners) to enable essential site functionality, enhance site navigation, analyze site usage, personalization, and assist in our advertising and marketing efforts and provide social media features, for which we may share cookie data with our third-party partners. You can update or manage your settings at any time. To learn more, see our [Cookie Policy](https://www.opentext.com/about/cookie-policy)

Reject All

Accept All

Summary (https://www.opentext.com/about/cookie-policy)

A security audit identified a privilege escalation vulnerability in Operations Agent on Windows. Under specific conditions Operations Agent may run executables from specific writeable locations. CVE-2026-2123

Operations Agent (OA)
(/s/topic/0TO8e00000YC1wGA...

Trending Articles


[The event with ID 'xxxxxxx-xxxx-xxxx-xxxxxxxxxxxx' does not exist or is not accessible by the user \(/s/article/KM000037803\)](#)

[How is Uptime calculated in quick report \(/s/article/KM000039589\)](#)

[Chromium based browser Manifest v2 deprecation \(/s/article/KM000030698\)](#)

[List of latest available hotfixes for supported Content Manager versions \(/s/article/KM000006342\)](#)

[Get "RPC: Failed to create RPC client" error when monitoring UNIX Resource in LoadRunner Host server \(/s/article/KM000039591\)](#)

[Files \(/s/relatedlist/ka0Q4000000GpbFIAS/AttachedContentDocuments\)](#) 



<https://www.linkedin.com/company/opentext>  <https://twitter.com/OpenText>  <https://www.youtube.com/user/opentextcorp>

Powered by OpenText TeamSite

We use cookies and similar technologies (including third party cookies from our partners) to enable essential site functionality, enhance site navigation, analyze site usage, personalization, and assist in our advertising and marketing efforts and provide social media features, for which we may share cookie data with our third-party partners. You can update or manage your settings at any time. To learn more, see our [Cookie Policy \(https://www.opentext.com/about/cookie-policy\)](https://www.opentext.com/about/cookie-policy).