



# Privilege escalation vulnerability in Operations Agent

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

## Summary

<b>CVE</b>	CVE-2026-2123
<b>State</b>	PUBLISHED
<b>Assigner</b>	OpenText
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-31 18:16:46 UTC
<b>Updated</b>	2026-04-01 14:24:02 UTC
<b>Description</b>	A security audit identified a privilege escalation vulnerability in Operations Agent(<=OA 12.29) on Windows. Under specific

## Risk And Classification

**Primary CVSS:** v4.0 8.6 HIGH from security@opentext.com

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:P/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000130000 probability, percentile 0.021520000 (date 2026-04-02)

**Problem Types:** CWE-280 | CWE-280 CWE-280 Improper handling of insufficient permissions or privileges

Version	Source	Type	Score	Severity	Vector
4.0	security@opentext.com	Secondary	8.6	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:P/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E
4.0	CNA	CVSS	8.6	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:P/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H

## CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

Passive

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:P/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">OpenText</a>	<a href="#">Operations Agent</a>	affected OA 12.22 OA 12.29 custom	Windows

### References

Reference	Source	Link	Tags
<a href="https://portal.microfocus.com/s/article/KM000046068">portal.microfocus.com/s/article/KM000046068</a>	<a href="mailto:security@opentext.com">security@opentext.com</a>	<a href="https://portal.microfocus.com">portal.microfocus.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

### Additional Advisory Data

#### Solutions

**CNA:** The hotfix can be downloaded from the Marketplace <https://marketplace.opentext.com/itom/content/operations-agent-hotfix-for-cve-2026-2123-privilege-escalation/> for the OA versions mentioned below. 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

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](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**