



CVE-2026-33447

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

Summary

CVE	CVE-2026-33447
State	PUBLISHED
Assigner	Absolute
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-30 20:16:23 UTC
Updated	2026-05-05 02:26:55 UTC
Description	CVE-2026-33447 is a buffer overflow in a message parsing function of the Secure Access client prior to 14.50. Attackers wi

Risk And Classification

Primary CVSS: v4.0 2.3 LOW from SecurityResponse@netmotionsoftware.com

CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:P/VC:N/VI:L/VA:L/SC:N/SI:N/SA:N/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: 0.000480000 probability, percentile 0.147440000 (date 2026-05-04)

Problem Types: CWE-121 | CWE-121 CWE-121 Stack-based Buffer Overflow

Version	Source	Type	Score	Severity	Vector
4.0	SecurityResponse@netmotionsoftware.com	Secondary	2.3	LOW	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:P/VC:N/VI:L/
4.0	CNA	CVSS	2.3	LOW	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:P/VC:N/VI:L/
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

Present

Privileges Required

None

User Interaction

Passive

Confidentiality

Confidentiality

None

Integrity

Low

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:P/VC:N/VI:L/VA:L/SC:N/SI:N/SA:N/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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Absolute	Secure Access	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Absolute Software	Secure Access	affected 14.50 custom	Not specified

References

Reference	Source	Link
www.absolute.com/platform/security-information/vulnerability-archive/cve-2026-...	SecurityResponse@netmotionsoftware.com	www.absolute.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report