



CVE-2023-45160

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

Summary

CVE	CVE-2023-45160
State	PUBLIC
Assigner	security@1e.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-05 16:15:00 UTC
Updated	2023-11-02 10:15:00 UTC
Description	In the affected version of the 1E Client, an ordinary user could subvert downloaded instruction resource files, e.g., to substi

Risk And Classification

Problem Types: CWE-552

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	1e	Client	23.7.1.151	All	All	All
Application	1e	Client	8.1.2.62	All	All	All
Application	1e	Client	8.4.1.159	All	All	All
Application	1e	Client	9.0.1.88	All	All	All

References

Reference	Source	Link	Tags
Vulnerability Disclosure Policy - 1E	MISC	www.1e.com	
1e.my.site.com/s	MISC	1e.my.site.com	
CVE Info - 1E	MISC	www.1e.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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](#)

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