



CVE-2023-25292

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

Summary

CVE	CVE-2023-25292
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-27 01:15:00 UTC
Updated	2023-05-05 20:18:00 UTC
Description	Reflected Cross Site Scripting (XSS) in Intermesh BV Group-Office version 6.6.145, allows attackers to gain escalated privi

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Group-office	Group Office	6.6.145	All	All	All

References

Reference

[intermesh.com](#)

[GitHub - brainkok/CVE-2023-25292: Reflected Cross Site Scripting \(XSS\) in Intermesh BV Group-Office version 6.6.145, allows attackers to g](#)

[Group-Office open source groupware and CRM](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

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

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