



# CVE-2023-31468

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

## Summary

<b>CVE</b>	CVE-2023-31468
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-09-11 19:15:00 UTC
<b>Updated</b>	2023-09-14 17:58:00 UTC
<b>Description</b>	An issue was discovered in Inosoft VisiWin 7 through 2022-2.1 (Runtime RT7.3 RC3 20221209.5). The "%PROGRAMFILE

## Risk And Classification

**Problem Types:** CWE-276

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Inosoft	Visiwin 7	All	All	All	All

## References

Reference	Source	Link	Tags
Inosoft VisiWin 7 2022-2.1 Insecure Permissions / Privilege Escalation ≈ Packet Storm	MISC	<a href="https://packetstormsecurity.com">packetstormsecurity.com</a>	
Inosoft VisiWin 7 2022-2.1 - Insecure Folders Permissions - Windows local Exploit	MISC	<a href="https://www.exploit-db.com">www.exploit-db.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, c

No vendor comments have been submitted for this CVE.

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

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](#)**