



SolidCAM-GPPL-IDE: Path traversal in `inc` directive enables file probing and NTLM-hash leak

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2026-42213 |
| State | PUBLISHED |
| Assigner | GitHub_M |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-05-08 22:16:32 UTC |
| Updated | 2026-05-08 22:16:32 UTC |

Description SolidCAM-GPPL-IDE is an unofficial, independently developed extension, Postprocessor IDE for SolidCAM. From version 1

Risk And Classification

Primary CVSS: v4.0 5.1 MEDIUM from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/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

Problem Types: CWE-22 | CWE-200 | CWE-295 | CWE-918 | CWE-22 CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | CWE-200 CWE-200: Exposure of Sensitive Information to an Unauthorized Actor | CWE-295 CWE-295: Improper Certificate Validation | CWE-918 CWE-918: Server-Side Request Forgery (SSRF)

| Version | Source | Type | Score | Severity | Vector |
|---------|--------------------------------|-----------|-------|----------|--|
| 4.0 | security-advisories@github.com | Secondary | 5.1 | MEDIUM | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/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 |
| 4.0 | CNA | DECLARED | 5.1 | MEDIUM | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/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 v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

Active

Confidentiality

Low

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/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

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|--------|-------------------|----------------------------|---------------|
| CNA | Anzory | SolidCAM-GPPL-IDE | affected >= 1.0.0, < 1.0.2 | Not specified |

References

| Reference | Source | Link | Tags |
|---|--------------------------------|--------------|------|
| github.com/anzory/SolidCAM-GPPL-IDE/releases/tag/v1.0.2 | security-advisories@github.com | github.com | |
| github.com/anzory/SolidCAM-GPPL-IDE/security/advisories/GHSA-xvpx-9p39-g62m | security-advisories@github.com | github.com | |
| github.com/anzory/SolidCAM-GPPL-IDE/commit/9d0ba808afd143ede448026a5dc68... | security-advisories@github.com | github.com | |
| CVE Program record | CVE.ORG | www.cve.org | ca |
| NVD vulnerability detail | NVD | nvd.nist.gov | ca |

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

