



# deepinid plugin in dde-control-center is configured to skip TLS certificate verification when downloading avatar from remote server

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

## Summary

<b>CVE</b>	CVE-2026-35207
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-09 18:17:01 UTC
<b>Updated</b>	2026-04-09 18:17:01 UTC
<b>Description</b>	dde-control-center is the control panel of DDE, the Deepin Desktop Environment. plugin-deepinid is a plugin in dde-control-

## Risk And Classification

**Primary CVSS:** v3.1 5.4 MEDIUM from security-advisories@github.com

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

**Problem Types:** CWE-295 | CWE-295 CWE-295: Improper Certificate Validation

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N
3.1	CNA	DECLARED	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

None

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Linuxdeepin	Dde-control-center	affected >= 6.1.35, < 6.1.80	Not specified
CNA	Linuxdeepin	Dde-control-center	affected >= 5.5.3, < 5.9.9	Not specified
CNA	Linuxdeepin	Deepin-deepinid-plugin	affected >= 2.0.1, <= 2.0.9	Not specified

### References

Reference	Source	Link	Tags
github.com/linuxdeepin/dde-control-center/commit/6fc206120be28d9eef7d722...	security-advisories@github.com	github.com	
github.com/linuxdeepin/dde-control-center/pull/3146	security-advisories@github.com	github.com	
github.com/linuxdeepin/developer-center/security/advisories/GHSA-jf2h-4v...	security-advisories@github.com	github.com	
github.com/linuxdeepin/dde-control-center/commit/cd95b054ff10a35bc928443...	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

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](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)