



# Privilege Bypass in PcManager

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2026-31369
<b>State</b>	PUBLISHED
<b>Assigner</b>	Honor
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-21 07:16:09 UTC
<b>Updated</b>	2026-04-21 07:16:09 UTC
<b>Description</b>	PcManager is affected by type privilege bypass, successful exploitation of this vulnerability may affect service availability

## Risk And Classification

**Primary CVSS:** v3.1 3.2 LOW from 3836d913-7555-4dd0-a509-f5667fdf5fe4

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

Version	Source	Type	Score	Severity	Vector
3.1	3836d913-7555-4dd0-a509-f5667fdf5fe4	Secondary	3.2	LOW	CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:C/C:N/I:N/A:L
3.1	CNA	CVSS	3.2	LOW	CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:C/C:N/I:N/A:L

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

None

Integrity

None

Availability

Low

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

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Honor</a>	<a href="#">PcManager</a>	affected 1.0.0.2 custom	Not specified

  

References			
Reference	Source	Link	Tags
<a href="http://www.honor.com/global/security/CVE-2026-31369">www.honor.com/global/security/CVE-2026-31369</a>	3836d913-7555-4dd0-a509-f5667fdf5fe4	<a href="http://www.honor.com">www.honor.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	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](https://cve.report/api)

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