



Nano: nano: local attacker can inject malicious .desktop launcher due to insecure directory permissions

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

Summary

CVE CVE-2026-6842

State PUBLISHED

Assigner redhat

Source Priority CVE Program / NVD first with legacy fallback

Published 2026-04-22 08:16:13 UTC

Updated 2026-04-22 08:16:13 UTC

Description A flaw was found in nano. In environments with permissive umask settings, a local attacker can exploit incorrect directory permissions to inject a malicious .desktop launcher.

Risk And Classification

Primary CVSS: v3.1 2.5 LOW from secalert@redhat.com

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

Problem Types: CWE-732 | CWE-732 Incorrect Permission Assignment for Critical Resource

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Primary	2.5	LOW	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N
3.1	CNA	CVSS	2.5	LOW	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat Enterprise Linux 10	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 6	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 7	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9	Not specified	Not specified
CNA	Red Hat	Red Hat OpenShift Container Platform 4	Not specified	Not specified

References

Reference	Source	Link	Tags
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
access.redhat.com/security/cve/CVE-2026-6842	secalert@redhat.com	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Red Hat would like to thank Michał Majchrowicz, Marcin Wyczechowski (AFINE Team) for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-04-13T00:00:00.000Z	Reported to Red Hat.
CNA	2026-04-13T00:00:00.000Z	Made public.

Workarounds

CNA: Ensure that the system's umask is configured to a secure value, such as ``0022`` or ``0077``, to prevent the creation of world-writable directories. This can be set system-wide in ``/etc/profile`` or ``/etc/bashrc``, or for individual users in their ``~/.bashrc`` or ``~/.profile``. A secure umask will ensure that newly created directories, including ``~/local`` by ``nano``, have appropriate permissions.

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](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)