



Firewalld: firewalld: local unprivileged user can modify firewall state due to d-bus setter mis-authorization

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2026-4948 |
| State | PUBLISHED |
| Assigner | redhat |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-03-27 06:16:39 UTC |
| Updated | 2026-03-30 13:26:29 UTC |

Description A flaw was found in firewalld. A local unprivileged user can exploit this vulnerability by mis-authorizing two runtime D-Bus (C

Risk And Classification

Primary CVSS: v3.1 5.5 MEDIUM from secalert@redhat.com

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

EPSS: 0.000190000 probability, percentile 0.050300000 (date 2026-04-01)

Problem Types: CWE-279 | CWE-279 Incorrect Execution-Assigned Permissions

| Version | Source | Type | Score | Severity | Vector |
|---------|---------------------|---------|-------|----------|--|
| 3.1 | secalert@redhat.com | Primary | 5.5 | MEDIUM | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N |
| 3.1 | CNA | CVSS | 5.5 | MEDIUM | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N |

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

None

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/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 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-2026-4948 | 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 Asim Viladi Oglu Manizada for reporting this issue. (en)

Additional Advisory Data

| Source | Time | Event |
|--------|--------------------------|----------------------|
| CNA | 2026-03-27T04:44:51.806Z | Reported to Red Hat. |
| CNA | 2026-03-27T00:00:00.000Z | Made public. |

Workarounds

CNA: To mitigate this issue, ensure that the firewalld desktop policy is not active on systems where local unprivileged user access is a concern. If firewalld is not required, it can be disabled. Disabling firewalld may impact network services that rely on it. To disable firewalld: `sudo systemctl stop firewalld` `sudo systemctl disable firewalld` A system restart or service reload may be required for changes to take full effect.

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

There are currently no legacy CVE 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](#).

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