



# CVE-2016-5410

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

## Summary

<b>CVE</b>	CVE-2016-5410
<b>State</b>	PUBLISHED
<b>Assigner</b>	redhat
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-04-19 14:59:00 UTC
<b>Updated</b>	2025-04-20 01:37:25 UTC
<b>Description</b>	firewalld.py in firewalld before 0.4.3.3 allows local users to bypass authentication and modify firewall configurations via the (

## Risk And Classification

**Primary CVSS:** v3.0 5.5 MEDIUM from nvd@nist.gov

**CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N**

**Problem Types:** CWE-287 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	5.5	MEDIUM	<b>CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N</b>
2.0	nvd@nist.gov	Primary	2.1		<b>AV:L/AC:L/Au:N/C:N/I:P/A:N</b>

## CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

None

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N

### CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:L/AC:L/Au:N/C:N/I:P/A:N

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Firewalld	Firewalld	All	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

### References

Reference	Source
Firewalld CVE-2016-5410 Security Bypass Vulnerability	af854a3a-2127-422b-9
oss-security - firewalld: Firewall configuration can be modified by any logged in user	af854a3a-2127-422b-9
Firewalld: Improper authentication methods (GLSA 201701-70) — Gentoo security	af854a3a-2127-422b-9
[SECURITY] Fedora 25 Update: firewalld-0.4.3.3-1.fc25 - package-announce - Fedora Mailing-Lists	af854a3a-2127-422b-9
1360135 – (CVE-2016-5410) CVE-2016-5410 firewalld: Firewall configuration can be modified by any logged in user	af854a3a-2127-422b-9
Red Hat Customer Portal	af854a3a-2127-422b-9

firewalld 0.4.3.3 release   firewalld	af854a3a-2127-422b-9
[SECURITY] Fedora 24 Update: firewalld-0.4.3.3-1.fc24 - package-announce - Fedora Mailing-Lists	af854a3a-2127-422b-9
[SECURITY] Fedora 25 Update: firewalld-0.4.3.3-1.fc25 - package-announce - Fedora Mailing-Lists	MITRE
[SECURITY] Fedora 24 Update: firewalld-0.4.3.3-1.fc24 - package-announce - Fedora Mailing-Lists	MITRE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[710510](#) Gentoo Linux Firewalld Improper authentication methods Vulnerability (GLSA 201701-70)

© [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](#)