



# CVE-2022-2127

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2022-2127
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-07-20 15:15:00 UTC
<b>Updated</b>	2024-01-30 16:15:00 UTC
<b>Description</b>	An out-of-bounds read vulnerability was found in Samba due to insufficient length checks in winbindd_pam_auth_crap.c. W

## Risk And Classification

**Problem Types:** CWE-125

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	12.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	37	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	38	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	9.0	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	All	All	All	All

## References

Reference	Source	Link	Ta
Red Hat		<a href="#">access.redhat.com</a>	
[SECURITY] Fedora 38 Update: samba-4.18.5-0.fc38 - package-announce - Fedora Mailing-Lists	MISC	<a href="#">lists.fedoraproject.org</a>	
cve-details	MISC	<a href="#">access.redhat.com</a>	
Debian -- Security Information -- DSA-5477-1 samba	MISC	<a href="#">www.debian.org</a>	
Red Hat		<a href="#">access.redhat.com</a>	
Samba - Security Announcement Archive	MISC	<a href="#">www.samba.org</a>	

Red Hat			<a href="https://access.redhat.com">access.redhat.com</a>	
Red Hat			<a href="https://access.redhat.com">access.redhat.com</a>	
July 2023 Samba Vulnerabilities in NetApp Products   NetApp Product Security	MISC		<a href="https://security.netapp.com">security.netapp.com</a>	
2222791 – (CVE-2022-2127) CVE-2022-2127 samba: out-of-bounds read in winbind AUTH_CRAP	MISC		<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>	
[SECURITY] Fedora 37 Update: samba-4.17.10-0.fc37 - package-announce - Fedora Mailing-Lists	MISC		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
CVE Program record	CVE.ORG		<a href="https://www.cve.org">www.cve.org</a>	car
NVD vulnerability detail	NVD		<a href="https://nvd.nist.gov">nvd.nist.gov</a>	car

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

<a href="#">161079</a> Oracle Enterprise Linux Security Update for samba (ELSA-2023-6667)
<a href="#">161138</a> Oracle Enterprise Linux Security Update for samba (ELSA-2023-7139)
<a href="#">199593</a> Ubuntu Security Notification for Samba Vulnerabilities (USN-6238-1)
<a href="#">242329</a> Red Hat Update for samba security (RHSA-2023:6667)
<a href="#">242428</a> Red Hat Update for samba security (RHSA-2023:7139)
<a href="#">242787</a> Red Hat Update for samba (RHSA-2024:0580)
<a href="#">242852</a> Red Hat Update for samba (RHSA-2024:0423)
<a href="#">284336</a> Fedora Security Update for samba (FEDORA-2023-76c06c8576)
<a href="#">284369</a> Fedora Security Update for samba (FEDORA-2023-bcd91bfcd3)
<a href="#">355878</a> Amazon Linux Security Advisory for samba : ALAS2023-2023-316
<a href="#">356750</a> Amazon Linux Security Advisory for samba : ALAS2-2023-2367
<a href="#">356781</a> Amazon Linux Security Advisory for samba : ALAS-2023-1896
<a href="#">379622</a> Alibaba Cloud Linux Security Update for evolution-mapi (ALINUX3-SA-2024:0037)
<a href="#">6000221</a> Debian Security Update for samba (DSA 5477-1)
<a href="#">6000543</a> Debian Security Update for samba (DSA 5647-1)
<a href="#">673521</a> EulerOS Security Update for samba (EulerOS-SA-2023-2907)
<a href="#">673550</a> EulerOS Security Update for samba (EulerOS-SA-2023-3157)
<a href="#">673600</a> EulerOS Security Update for samba (EulerOS-SA-2023-2869)
<a href="#">673784</a> EulerOS Security Update for samba (EulerOS-SA-2023-3229)
<a href="#">673831</a> EulerOS Security Update for samba (EulerOS-SA-2023-2852)

673954 EulerOS Security Update for samba (EulerOS-SA-2023-2888)
674025 EulerOS Security Update for samba (EulerOS-SA-2023-3194)
691226 Free Berkeley Software Distribution (FreeBSD) Security Update for samba (441e1e1a-27a5-11ee-a156-080027f5fec9)
710873 Gentoo Linux Samba Multiple Vulnerabilities (GLSA 202402-28)
754194 SUSE Enterprise Linux Security Update for samba (SUSE-SU-2023:2888-1)
754195 SUSE Enterprise Linux Security Update for samba (SUSE-SU-2023:2887-1)
754222 SUSE Enterprise Linux Security Update for samba (SUSE-SU-2023:3017-1)
754225 SUSE Enterprise Linux Security Update for samba (SUSE-SU-2023:3060-1)
754284 SUSE Enterprise Linux Security Update for samba (SUSE-SU-2023:3358-1)
755893 SUSE Enterprise Linux Security Update for samba (SUSE-SU-2023:2929-1)
755894 SUSE Enterprise Linux Security Update for samba (SUSE-SU-2023:2930-1)
941384 AlmaLinux Security Update for samba (ALSA-2023:6667)
941423 AlmaLinux Security Update for samba (ALSA-2023:7139)

© [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](#)