



CVE-2021-44141

Published on: Not Yet Published

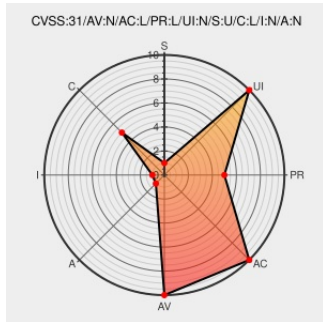
Last Modified on: 02/28/2022 05:50:05 PM UTC

CVE-2021-44141

Source: Mitre

Source: Nist

Print: PDF



Certain versions of [Fedora](#) from [Fedoraproject](#) contain the following vulnerability:

All versions of Samba prior to 4.15.5 are vulnerable to a malicious client using a server symlink to determine if a file or directory exists in an area of the server file system not exported under the share definition. SMB1 with unix extensions has to be enabled in order for this attack to succeed.

CVE-2021-44141 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **4.3 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	LOW	NONE	NONE

CVSS2 Score: **3.5 - LOW**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Samba - Security Announcement Archive	Mitigation Vendor Advisory www.samba.org	S MISC www.samba.org/samba/security/CVE-2021-44141.html

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

- [240286](#) Red Hat Update for samba security (RHSA-2022:1756)
- [240314](#) Red Hat Update for samba security (RHSA-2022:2074)
- [282312](#) Fedora Security Update for samba (FEDORA-2022-50da406d40)
- [282317](#) Fedora Security Update for samba (FEDORA-2022-055efdd9dc)
- [690784](#) Free Berkeley Software Distribution (FreeBSD) Security Update for samba (8579074c-839f-11ec-a3b2-005056a311d1)
- [751680](#) OpenSUSE Security Update for samba (openSUSE-SU-2022:0283-1)
- [751683](#) SUSE Enterprise Linux Security Update for samba (SUSE-SU-2022:0323-1)
- [751994](#) SUSE Enterprise Linux Security Update for samba (SUSE-SU-2022:0283-1)
- [901502](#) Common Base Linux Mariner (CBL-Mariner) Security Update for samba (8610)
- [940520](#) AlmaLinux Security Update for samba (ALSA-2022:2074)








Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Redhat	Storage	3.0	All	All	All
Application	Samba	Samba	All	All	All	All
cpe:2.3:o:fedoraproject:fedora:34:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:35:*:*:*:*:*:						
cpe:2.3:a:redhat:storage:3.0:*:*:*:*:*:						
cpe:2.3:a:samba:samba:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@softek_jp	Samba に共有定義の外側にあるファイルまたはディレクトリの存在を特定される問題 (CVE-2021-44141) [41192] sid.softek.jp/content/show/4... #SIDfm #脆弱性情報	2022-02-01 06:04:46

 @PSantavy	Samba - security flaws fixed samba.org/samba/latest_n... CVE-2021-44141, CVE-2021-44142, CVE-2022-0336 #CVE-2022-44142... twitter.com/i/web/status/1...	2022-02-01 20:15:19
 @OpenBSD_ports	jca@ modified net/samba: SECURITY UPDATE to samba-4.15.5 Fixes for CVE-2021-44141, CVE-2021-44142 and CVE-2022-0336... twitter.com/i/web/status/1...	2022-02-02 12:55:25
 @omokazuki	SIOSセキュリティブログを更新しました。 Sambaの脆弱性情報(Critical: CVE-2021-44142, Important: CVE-2022-0336, Medium: CVE-2021-44141)と新バージョン... twitter.com/i/web/status/1...	2022-02-02 22:05:50
 @ikatzsolutions	Samba admins please note released security updates: samba.org/samba/security... samba.org/samba/security..... twitter.com/i/web/status/1...	2022-02-03 07:07:25
 @qualys	#Qualys released version 2 of its Unified Dashboard on Samba OOB Heap Read/Write CVE-2021-44141, CVE-2021-44142,... twitter.com/i/web/status/1...	2022-02-03 22:48:07
 @hackerfantastic	A trifecta of interesting vulnerabilities in Samba service, tons of stuff vulnerable. samba.org/samba/security... (path... twitter.com/i/web/status/1...	2022-02-04 16:03:59
 /r/blueteamsec	Heads up Samba users	2022-02-01 19:04:16

[← Previous ID](#)

[Next ID→](#)

© CVE.report 2022   |

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](#)