



# CVE-2021-44142

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

## Summary

<b>CVE</b>	CVE-2021-44142
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-02-21 15:15:00 UTC
<b>Updated</b>	2023-11-07 03:39:00 UTC
<b>Description</b>	The Samba vfs_fruit module uses extended file attributes (EA, xattr) to provide "...enhanced compatibility with Apple SMB c

## Risk And Classification

**Problem Types:** CWE-125 | CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	20.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	21.10	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	11.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	34	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	35	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Codeready Linux Builder</a>	-	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 Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	8.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	8.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Ibm Z Systems</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Ibm Z Systems</a>	8.0	All	All	All

Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux For Power Big Endian	7.0	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian	7.0	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian	8.0	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian Eus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian Eus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux For Scientific Computing	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Resilient Storage	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	8.1	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Update Services For Sap Solutions	8.1	All	All	All
Operating System	Redhat	Enterprise Linux Server Update Services For Sap Solutions	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Update Services For Sap Solutions	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Application	Redhat	Gluster Storage	3.5	All	All	All
Application	Redhat	Virtualization Host	4.0	All	All	All
Application	Samba	Samba	All	All	All	All
Application	Synology	Diskstation Manager	All	All	All	All

## References

Reference	Source	Link
Zero Day Initiative — CVE-2021-44142: Details on a Samba Code Execution Bug Demonstrated at Pwn2Own Austin	MISC	<a href="http://www.zerodayinitiative.com/blog/2021/10/20/cve-2021-44142-details-on-a-samba-code-execution-bug-demonstrated-at-pwn2own-austin">www.zerodayinitiative.com</a>
Samba - Security Announcement Archive	CONFIRM	<a href="http://www.samba.org/security/announcements/">www.samba.org/security/announcements/</a>
VU#119678 - Samba vfs_fruit module insecurely handles extended file attributes	CERT-VN	<a href="https://kb.cert.org/vuls/id/119678">kb.cert.org</a>
Samba: Multiple Vulnerabilities (GLSA 202309-06) — Gentoo security		<a href="https://security.gentoo.org/glsa/202309-06">security.gentoo.org</a>
14914 – (CVE-2021-44142) CVE-2021-44142 [SECURITY] Out-of-Bound Read/Write on Samba vfs_fruit module	CONFIRM	<a href="https://bugzilla.redhat.com/show_bug.cgi?id=14914">bugzilla.redhat.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org/CVERecord?id=CVE-2021-44142">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov/vuln/detail/CVE-2021-44142">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

159607 Oracle Enterprise Linux Security Update for samba (ELSA-2022-0328)

159608 Oracle Enterprise Linux Security Update for samba (ELSA-2022-0332)

179066 Debian Security Update for samba (DSA 5071-1)

183878 Debian Security Update for samba (CVE-2021-44142)

198650 Ubuntu Security Notification for Samba Vulnerability (USN-5260-2)

198651 Ubuntu Security Notification for Samba Vulnerabilities (USN-5260-1)

240046 Red Hat Update for samba (RHSA-2022:0332)

240047 Red Hat Update for samba (RHSA-2022:0331)

240049 Red Hat Update for samba (RHSA-2022:0328)

240050 Red Hat Update for samba (RHSA-2022:0330)

240068 Red Hat Update for samba (RHSA-2022:0458)

240069 Red Hat Update for samba (RHSA-2022:0457)

240420 Red Hat Update for samba (RHSA-2022:0664)

257150 CentOS Security Update for samba (CESA-2022:0328)

282312 Fedora Security Update for samba (FEDORA-2022-50da406d40)

282317 Fedora Security Update for samba (FEDORA-2022-055efdd9dc)

296057 Oracle Solaris 11.4 Support Repository Update (SRU) 44.113.4 Missing (bulletinapr2022)

353164 Amazon Linux Security Advisory for samba : ALAS2-2022-1746

353170 Amazon Linux Security Advisory for samba : ALAS-2022-1564

354310 Amazon Linux Security Advisory for samba : ALAS2022-2022-022

354496 Amazon Linux Security Advisory for samba : ALAS2022-2022-224

354550 Amazon Linux Security Advisory for samba : ALAS-2022-224

376944 Alibaba Cloud Linux Security Update for samba (ALINUX2-SA-2022:0009)

376950 Alibaba Cloud Linux Security Update for samba (ALINUX3-SA-2022:0010)

38857 Samba Out-Of-Bounds Heap Read/Write Vulnerability

501490 Alpine Linux Security Update for samba

501779 Alpine Linux Security Update for samba

<a href="#">502620</a> Alpine Linux Security Update for samba
<a href="#">503810</a> Alpine Linux Security Update for samba
<a href="#">671442</a> EulerOS Security Update for samba (EulerOS-SA-2022-1459)
<a href="#">671468</a> EulerOS Security Update for samba (EulerOS-SA-2022-1438)
<a href="#">671569</a> EulerOS Security Update for samba (EulerOS-SA-2022-1586)
<a href="#">671587</a> EulerOS Security Update for samba (EulerOS-SA-2022-1551)
<a href="#">671623</a> EulerOS Security Update for samba (EulerOS-SA-2022-1666)
<a href="#">671635</a> EulerOS Security Update for samba (EulerOS-SA-2022-1652)
<a href="#">671687</a> EulerOS Security Update for samba (EulerOS-SA-2022-1763)
<a href="#">690784</a> Free Berkeley Software Distribution (FreeBSD) Security Update for samba (8579074c-839f-11ec-a3b2-005056a311d1)
<a href="#">710751</a> Gentoo Linux Samba Multiple Vulnerabilities (GLSA 202309-06)
<a href="#">730392</a> Palo Alto Networks (PAN-OS) Impact of the Samba Vulnerability (PAN-187873)
<a href="#">751674</a> SUSE Enterprise Linux Security Update for samba (SUSE-SU-2022:0251-1)
<a href="#">751675</a> SUSE Enterprise Linux Security Update for samba (SUSE-SU-2022:0271-1)
<a href="#">751676</a> SUSE Enterprise Linux Security Update for samba (SUSE-SU-2022:0284-1)
<a href="#">751677</a> SUSE Enterprise Linux Security Update for samba (SUSE-SU-2022:0287-1)
<a href="#">751678</a> OpenSUSE Security Update for samba (openSUSE-SU-2022:0287-1)
<a href="#">751680</a> OpenSUSE Security Update for samba (openSUSE-SU-2022:0283-1)
<a href="#">751681</a> OpenSUSE Security Update for samba (openSUSE-SU-2022:0284-1)
<a href="#">751683</a> SUSE Enterprise Linux Security Update for samba (SUSE-SU-2022:0323-1)
<a href="#">751994</a> SUSE Enterprise Linux Security Update for samba (SUSE-SU-2022:0283-1)
<a href="#">901364</a> Common Base Linux Mariner (CBL-Mariner) Security Update for samba (8611)
<a href="#">940442</a> AlmaLinux Security Update for samba (ALSA-2022:0332)
<a href="#">960106</a> Rocky Linux Security Update for samba (RLSA-2022:332)
<a href="#">960866</a> Rocky Linux Security Update for samba (RLSA-2022:0332)

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](#)**