



Bug 2305954 (CVE-2020-25720) - CVE-2020-25720 samba: check attribute access rights for LDAP adds of computers

Keywords:

Reported: 2024-08-20 07:40 UTC by Dhananjay Arunesh

Status: NEW

Modified: 2026-04-27 21:01 UTC ([History](#))

Alias: CVE-2020-25720

CC List: 5 users ([show](#))

Product: Security Response

Fixed In Version:

Component: vulnerability

Clone Of:

Environment:

Version: unspecified

Last Closed:

Embargoed:

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On:

Blocks:

TreeView+ [depends on](#) / [blocked](#)

Attachments ([Terms of Use](#))

Dhananjay Arunesh 2024-08-20 07:40:44 UTC

[Description](#)

A delegated administrator who can create objects in Active Directory, can write to all attributes in that new object, including after the object is created because they own the object. This includes some security-sensitive attributes (less in Samba than in Windows).

Because these rights are due to there being no ACL at creation time and later being the nebulous 'creator owner', the implication that the delegated administrator retains significant rights may not be well understood.


Behaviour removing the implicit rights of creating users to write to all attributes is off by default in Samba and Windows (see CVE-2021-42291)

)

(As mentioned in the bug, we developed some other protections for this that landed in the other CVEs, which is why this one didn't get the full security notice treatment).

The details of how to turn this protection on are at:

<https://support.microsoft.com/en-us/topic/kb5008383-active-directory-permissions-updates-cve-2021-42291-536d5555-ffba-4248-a60e-d6cbc849cde1>

Guenther Deschner  2024-08-22 19:54:04 UTC

[Comment 1](#)

As outlined in <https://access.redhat.com/security/cve/CVE-2020-25720> this is a Samba AD only problem and Samba AD is not built in any Red Hat product and thus this CVE is not relevant for RHEL or RHGS at all.

Note

You need to [log in](#) before you can comment on or make changes to this bug.

