### Security Advisory 2022-056

# Critical Vulnerabilities In Samba

***July 29, 2022 — v1.0***

**TLP:WHITE**

*History:*

- *29/07/2022 — v1.0 – Initial publication*

## Summary

On June 27, 2022, The Samba Team has released security updates to address several vulnerabilities in their product. Exploitation of these vulnerabilities may allow an attacker to cause a DoS condition, data leakage, or even to take control of all the domain. [1][2]

## Technical Details

The security release addresses the following defects:

- **CVE-2022-2031** - Samba AD users can bypass certain restrictions associated with changing passwords.

  The KDC and the kpasswd service share a single account and set of keys, allowing them to decrypt each other's tickets. This also makes the two services susceptible to confusion. A user who has been requested to change their password can exploit this to obtain and use tickets to other services. [3]

- **CVE-2022-32744** - Samba AD users can forge password change requests for any user.

  The KDC accepts kpasswd requests encrypted with any key known to it. By encrypting forged kpasswd requests with its own key, a user can change the passwords of other users, enabling full domain take over. [4]

- **CVE-2022-32745** - Samba AD users can crash the server process with an LDAP add or modify request.

  Samba AD users can cause the server to access uninitialised data with an LDAP add or modify request due to incorrect values used as the limit for a loop and as the 'count' parameter to memcpy(), usually resulting in a segmentation fault. [5]

- **CVE-2022-32746** - Samba AD users can induce a use-after-free in the server process with an LDAP add or modify request.

  The AD DC database audit logging module can be made to access LDAP message values that have been freed by a preceding database module, resulting in a use-after- free. This is only possible when modifying certain privileged attributes, such as userAccountControl. When the database audit logging module subsequently logs the details of the original

message, it will access this freed data, generally resulting in corrupted log output or a crash. [6]

- **CVE-2022-32742** - Server memory information leak via SMB1.

  Please note that only versions of Samba prior to 4.11.0 are vulnerable to this bug by default. Samba versions 4.11.0 and above disable SMB1 by default, and will only be vulnerable if the administrator has deliberately enabled SMB1 in the smb.conf file. All versions of Samba with SMB1 enabled are vulnerable to a server memory information leak bug over SMB1 if a client can write data to a share. Some SMB1 write requests were not correctly range checked to ensure the client had sent enough data to fulfil the write, allowing server memory contents to be written into the file (or printer) instead of client supplied data. The client cannot control the area of the server memory that is written to the file (or printer). [7]

## Recommendations

CERT-EU strongly recommend upgrading samba to the last available version. Also, CERT-EU strongly discourages the use of SMB1.

## References


[1] https://www.samba.org/samba/history/samba-4.16.4.html

[2] https://nakedsecurity.sophos.com/2022/07/27/critical-samba-bug-could-let-anyone-become-domain-admin-patch-now/

[3] https://www.samba.org/samba/security/CVE-2022-2031.html

[4] https://www.samba.org/samba/security/CVE-2022-32744.html

[5] https://www.samba.org/samba/security/CVE-2022-32745.html

[6] https://www.samba.org/samba/security/CVE-2022-32746.html

[7] https://www.samba.org/samba/security/CVE-2022-32742.html