Security Advisory 2022-008

Critical Vulnerability in Samba

February 1, 2022 — v1.0

TLP:WHITE

History:

- *01/02/2022 — v1.0 – Initial publication*

Summary

On January 31, Samba has issued advisories and software updates [1] to address multiple vulnerabilities one of which, identified as `CVE-2021-44142`, could lead to Remote Code Execution with `root` privileges. It is recommended to update as soon as possible.

Technical Details

The vulnerability `CVE-2021-44142`, with a severity score of 9.9 out of 10, is an out-of-bounds heap read-write vulnerability that allows remote attackers to execute arbitrary code as `root` on affected Samba installations [2].

The specific flaw exists within the parsing of Extended Attributes (EA) metadata when opening files in `smbd`.

Access as a user that has write access to a file's extended attributes is required to exploit this vulnerability. Note that this could be a guest or unauthenticated user if such users are allowed write access to file extended attributes.

Affected Products

All versions of Samba prior to `4.13.17` are vulnerable when Samba has the VFS module `vfs_fruit` enabled in its default configuration. This means that the following options are configured as follows: `fruit:metadata=netatalk` or `fruit:resource=file`. If both options are set to different settings than the default values, the system is not affected by the security issue.

Recommendations

Samba team and CERT-EU strongly recommend upgrading Samba to the latest version as soon as possible.

Workaround

As a temporary workaround, one can remove the `fruit` VFS module from the list of configured VFS objects in any `vfs objects` line in the Samba configuration `smb.conf`.

Note that changing the VFS module settings `fruit:metadata` or `fruit:resource` to use the unaffected setting causes all stored information to be inaccessible.

References

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

[2] https://www.samba.org/samba/security/CVE-2021-44142.html