NCSC

National Cyber Security Centre

2202020100-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Alert

Critical Vulnerability in Samba

CVE-2021-44142 - CVSSv3 - 9.9

2022-02-02

Status: TLP-WHITE

This document is classified using Traffic Light Protocol. Recipients may share TLP-WHITE *information freely, without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.*

Description

A critical vulnerability exists in Samba (CVE-2021-44142, CVSS-9.9), that allows remote attackers to execute arbitrary code on affected installations of Samba as root.

Samba is the standard Windows interoperability suite for Linux/Unix, which is a re-implementation of the Server Message Block (SMB) for file and print services. It typically runs on Unix and Unix-like systems such as Linux and macOS systems. It allows network administrators to configure, integrate, and set up equipment either as a domain controller (DC) or domain member, and to communicate with Windows-based clients.

All versions of Samba prior to 4.13.17 are vulnerable to an out-of-bounds heap read write vulnerability that allows remote attackers to execute arbitrary code as root on affected Samba installations that use the VFS module, vfs_fruit.

The specific flaw exists within the parsing of 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.

The problem in vfs_fruit exists in the default configuration of the fruit VFS module using **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.

Products Affected

All versions of Samba prior to 4.13.17

Recommendations

Patches addressing this vulnerability have been posted to:
https://www.samba.org/samba/security/
Trend Micro have also released a blog regarding this issue:
https://www.trendmicro.com/en_us/research/22/b/the-samba-vulnerability-what-is-cve-2021-44142-and-how-to-fix-it.html

Additionally, Samba 4.13.17, 4.14.12 and 4.15.5 have been issued as security releases to correct the defect. Samba administrators are advised to upgrade to these releases or apply the patch as soon as possible.

There is a workaround available, 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 and will make it appear to macOS clients as if the information is lost.

DISCLAIMER: *This document is provided "as is" without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.*

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie