Hive Pro

THREAT ADVISORY

Critical Samba vulnerability allows remote code execution as root

TA2022023

Threat Level AMBER

Publish Date – Feb 2, 2022

A critical vulnerability identified in Samba allows an attacker to execute remote code and gain access to the vulnerable system as root. Samba installations that use VFS module " vfs_fruit" are impacted by this vulnerability.

An out-of-bounds heap read/write vulnerability exists in the parsing of Extended Attributes (EA) metadata while opening files in smbd. To exploit this issue, an attacker requires to have the write access to a file's extended attributes. According to samba, one possible workaround is to “Remove the "fruit" VFS module from the list of configured VFS objects in any "vfs objects" line in the Samba configuration smb.conf.” Organizations should update their software to 4.13.17 to patch this vulnerability.

Potential Mitre Att&ck TTPs are :
TA0005: Defense Evasion
TA0004: Privilege Escalation
T1564: Hide Artifacts
T1222: File and Directory Permissions Modification
T1068: Exploitation for Privilege Escalation
T1564.004: Hide Artifacts: NTFS File Attributes

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2021-44142	Samba prior to 4.13.17	cpe:2.3:a:samba:samba:*:*:*:*:*:*:*:*	Samba code execution vulnerability	CWE-787 CWE-125

Patch Link

https://www.samba.org/samba/history/security.html

References

https://www.samba.org/samba/security/CVE-2021-44142.html
https://www.cisa.gov/uscert/ncas/current-activity/2022/02/01/samba-releases-security-updates