UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00247

CRITICAL SAMBA 'FRUIT' BUG ALLOWS RCE

DATE ISSUED: 21st February 2022

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	**MEDIUM**	EASY

OVERVIEW

DEVCORE has discovered that the file-sharing and interop platform Samba, which allows Windows and Linux/Unix-based hosts to work together and affecting Red Hat, SUSE Linux and Ubuntu packages, could allow an attacker to perform a Remote Code Execution (RCE) attack with root user privileges.

BREAKDOWN

Samba facilitates sharing of files and print services with multi-platform devise on a common network. This out-of-bounds heap read/write vulnerability exists in the VFS module called "vfs_fruit". This module's purpose is to provide "enhanced compatibility with Apple SMB clients and interoperability with a Netatalk 3 AFP fileserver, through the use of extended file attribute (EA)." Two things that may prevent an attacker from proceeding are that if the module has different values to the default, they are not susceptible and that an attacker must have write access to the file's EA in order to be exploitable. The flaw specifically exists within "the parsing of metadata when opening files in smdb." Guests or unauthenticated users may be able to do this if write privileges are allowed on such account types. Once access was gained, attackers would be able to then move laterally across the network, read, modify, or destroy any files on the system and install other programs or malware. This critical vulnerability affects all versions of Samba prior to v4.13.17 and has received a 9.9 / 10 CVSS rating. It is being tracked as CVE-2021-44142

REMEDIATION STEPS

- Upgrade to the latest version of Samba v4.13.17, 4.14.12 and 4.15.5
- As a workaround 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.

REFERENCES & RESOURCES

Samba https://www.samba.org/samba/history/security.html
https://www.samba.org/samba/security/CVE-2021-44142.html
https://www.samba.org/samba/security/
Threatpost https://threatpost.com/samba-fruit-bug-rce-root-access/178141/