PHYS.ORG

Samba Repels Three Bugs with New Release

May 16 2007

Vulnerabilities have been uncovered in Samba, the popular file-and-print software.

The makers of Samba have patched a serious flaw in their open-source software that could be exploited remotely by hackers to inject code with nobody user privileges.

Samba is a suite of software for Unix and Linux operating systems that allows Windows clients to print files using a Linux or Unix machine.

The bug, as well as two other vulnerabilities, are addressed in Monday's release of Samba 3.0.25. In the case of the most critical flaw, Samba officials said in an advisory that unescaped user input parameters are passed as arguments to /bin/sh - a situation that allows for remote command execution.

Successful exploitation of this vulnerability allows an attacker to run arbitrary shell commands with the privileges of the nobody user, according to researchers at iDefense Labs, based in Sterling, Va.

"If the administrator has configured the Samba server to translate Windows account names to Unix account names, an unauthenticated user can run arbitrary shell commands," said Richard Howard, director of security intelligence at VeriSign. "The vulnerability is trivial to exploit even on systems that employ NX and ASLR."

Officials at iDefense noted that the vulnerability occurs within a nondefault configuration of Samba. Specifically, the "username map script" option must be defined in the smb.conf file, officials said.

A second problem is that Samba's NDR parsing can allow a user to send Microsoft Remote Procedure Call requests that will overwrite the heap space with user defined data, Samba officials warned in an advisory.

The final flaw patched in the release is a bug in the local SID/Name translation routines that can result in an attacker issuing SMB/CIFS protocol operations as root.

Copyright 2007 by Ziff Davis Media, Distributed by United Press International

Citation: Samba Repels Three Bugs with New Release (2007, May 16) retrieved 27 April 2024 from https://phys.org/news/2007-05-samba-repels-bugs.html