Serious Samba Problems

May 17 2007

Three critical bugs in the popular open-source program allow for system compromise.

Samba is a very popular free and open-source program for providing file-sharing services compatible with Microsoft Windows'. It is used extensively on Linux and other UNIX-variant operating systems.

The Samba team this week revealed three critical bugs in all versions of the software since 3.0, and released patches to bring it up to the new current (stable) release of 3.0.24. The three errors:

- Remote Command Injection Vulnerability - Unescaped user input parameters are passed as arguments to /bin/sh allowing for remote command execution.
- Multiple Heap Overflows Allow Remote Code Execution - Various bugs in Samba's NDR parsing can allow a user to send specially crafted MS-RPC requests that will overwrite the heap space with user defined data.
- Local SID/Name translation bug can result in user privilege elevation - An error in the software could allow elevation to root.

It's not typical for Samba servers to be exposed directly to the Internet with vulnerable protocols left unfiltered, but attacks could be launched

from within the network.

Samba is used in a wide variety of products, including NAS appliances. It's important to assess if you have any such products and to update them periodically to address problems such as these.