

Samba Arbitrary File Access Vulnerability

iDEFENSE Security Advisory 09.30.04:

I. BACKGROUND

Samba is an Open Source/Free Software suite that provides seamless file and print services to SMB/CIFS clients.

II. DESCRIPTION

Remote exploitation of an input validation vulnerability in Samba allows attackers to access files and directories outside of the specified share path.

Each file and directory name passed into Samba is converted and checked with the functions `unix_convert()` and `check_name()`. The main purpose of the `unix_convert()` routine is to convert names from the DOS namespace to Unix namespace. It calls `unix_clean_name()`, which in turn removes double slashes, leading `./` characters and `./` directory-traversal characters. `check_name()` does any final checks necessary to confirm the validity of the converted filename and calls `reduce_name()`, which in turn calls `unix_clean_name()` for a second time. The end result allows for an attacker to specify the realpath of any file on the computer.

Example:

`././././etc` is passed to `unix_clean_name()`. It becomes `./././etc`. The leading slash is then trimmed off to make `././etc`. It is then passed to `unix_clean_name()` again. The resulting string is `/etc`, which is an absolute path on the system.

III. ANALYSIS

Successful exploitation allows remote attackers to bypass the specified share restrictions to gain read, write and list access to files and directories under the privileges of the user. In situations where a public share is available, the attack can be performed by unauthenticated attackers.

An attacker does not need exploit code to exploit this vulnerability. The `smbclient` program can be used to request/write/list files using the `"get"`, `"put"` and `"dir"` commands, respectively.

IV. DETECTION

iDEFENSE has confirmed that Samba versions 3.0.2 and 2.2.9 are vulnerable. It is suspected that all versions of Samba are vulnerable.

V. WORKAROUND

Only allow trusted users/hosts to connect to samba shares.

VI. VENDOR RESPONSE

Samba 2.2.12 upgrade for Samba 2.2.x:

<http://us4.samba.org/samba/ftp/samba-2.2.12.tar.gz>

Samba 3.0.5 patch:

http://us4.samba.org/samba/ftp/patches/security/samba-3.0.5-reduce_name.patch

Samba 3.0.7 is not vulnerable.

VII. CVE INFORMATION

The Common Vulnerabilities and Exposures (CVE) project has assigned the names CAN-2004-0815 to these issues. This is a candidate for inclusion in the CVE list (<http://cve.mitre.org>), which standardizes names for security problems.

VIII. DISCLOSURE TIMELINE

09/22/2004 Initial vendor notification
09/22/2004 iDEFENSE clients notified
09/22/2004 Initial vendor response
09/30/2004 Coordinated public disclosure

IX. CREDIT

Karol Wieseck is credited with this discovery.