

[UNIX] Samba smbdc Security Descriptor Integer Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-12/0050.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/16/04

To: list@securiteam.com

Date: 16 Dec 2004 16:16:59 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Samba smbdc Security Descriptor Integer Overflow Vulnerability

SUMMARY

Samba is "an open source implementation of the SMB/CIFS protocol that allows Windows clients to use resources on non-Windows systems".

Remote exploitation of an integer overflow vulnerability in all versions of Samba's smbdc prior to and including 3.0.8 could allow an attacker to cause controllable heap corruption, leading to execution of arbitrary commands with root privileges.

DETAILS

Vulnerable Systems:

- * Samba version 3.0.8
- * Samba version 2.2.9

Immune Systems:

- * Samba version 3.0.9

To open a file on a Samba server, a client sends a sequence of SMB messages to the smbdc process. The message with the information on the file

Securiteam: [UNIX] Samba smbd Security Descriptor Integer Overflow Vulnerability

to open also contains a security descriptor, which is a list of access controls to apply to the file. The vulnerability specifically occurs in the allocation of memory to store these descriptors.

```
/*
 * Even if the num_aces is zero, allocate memory as there's a difference
 * between a non-present DACL (allow all access) and a DACL with no
ACE's
 * (allow no access).
 */
if((psa->ace = (SEC_ACE *)prs_alloc_mem(ps,sizeof(psa->ace[0]) *
(psa->num_aces+1))) == NULL)
    return False;
```

When more than 38347922 descriptors are requested, an integer overflow occurs resulting in less memory being allocated than was requested. sizeof(psa->ace[0]) is 112, or 0x70 in hex. 0x70x(38347922 + 1)=4294967376, or 0x100000050. This number is larger than can be stored in a 32-bit integer, so the bits that don't fit are removed, leaving 0x50, or 80 in decimal. As one descriptor is 112 bytes, an overflow of at least 32 bytes will occur.

An attacker could supply data to the server which would cause the heap to become corrupted in such a way as to cause arbitrary values to be written to arbitrary locations, eventually leading to code execution.

Analysis:

Successful remote exploitation allows an attacker to gain root privileges on a vulnerable system. In order to exploit this vulnerability an attacker would need to have credentials allowing them access to the a share. Unsuccessful exploitation attempts will cause the process serving the request to crash with signal 11, and may leave evidence of an attack in logs.

Vendor Response:

Patches for this issue are available at:

<<http://www.samba.org/samba/ftp/patches/security/samba-3.0.9-CAN-2004-1154.patch>>
<http://www.samba.org/samba/ftp/patches/security/samba-3.0.9-CAN-2004-1154.patch>

<<http://www.samba.org/samba/ftp/patches/security/samba-3.0.9-CAN-2004-1154.patch.asc>>
<http://www.samba.org/samba/ftp/patches/security/samba-3.0.9-CAN-2004-1154.patch.asc>

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1154>>
CAN-2004-1154

Disclosure Timeline:

12/02/2004 – Initial vendor notification
12/02/2004 – Initial vendor response
12/16/2004 – Coordinated public disclosure

Securiteam: [UNIX] Samba smbdc Security Descriptor Integer Overflow Vulnerability

ADDITIONAL INFORMATION

The information has been provided by
<mailto:idlabs-advisories@idefense.com> Greg MacManus of iDEFENSE.
The original article can be found at:
<<http://www.idefense.com/application/poi/display?id=165>>
<http://www.idefense.com/application/poi/display?id=165>

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.