

[UNIX] Linux 2.x smbfs Multiple Remote Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-11/0065.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 11/18/04

To: list@securiteam.com

Date: 18 Nov 2004 09:22:52 +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>

Linux 2.x smbfs Multiple Remote Vulnerabilities

SUMMARY

Linux is a clone of the operating system Unix, written from scratch by Linus Torvalds with assistance from a loosely-knit team of hackers across the Net. It aims towards POSIX and Single UNIX Specification compliance.

During an audit of the smb filesystem implementation within Linux several vulnerabilities were discovered ranging from out of bounds read accesses to kernel level buffer overflows.

To exploit any of these vulnerabilities an attacker needs control over the answers of the connected smb server. This could be achieved by man in the middle attacks or by taking over the smb server with the recently disclosed vulnerability in Samba 3.x

While any of these vulnerabilities can be easily used as remote denial of service exploits against Linux systems, it is unclear if it is possible for a skilled local or remote attacker to use any of the possible buffer overflows for arbitrary code execution in kernel space.

DETAILS

Securiteam: [UNIX] Linux 2.x smbfs Multiple Remote Vulnerabilities

Vulnerable Systems:

- * Linux version 2.4.27 and prior
- * Linux version Linux 2.7 up to 2.6.9

Immune Systems:

- * Linux version 2.4.28 and newer

01 – smb_proc_read(X) malicious data count overflow:

Affected Kernels: 2.4

When receiving the answer to a read(X) request the Linux 2.4 kernel trusts the returned data count and copies exactly that amount of bytes into the output buffer. This means any call to the read syscall on a smb filesystem could result in an overflow withing kernel memory if the connected smb server returns more data than requested. While this is a trivial to exploit DOS vulnerability it is unclear if it can be used by a skilled attacker to execute arbitrary code.

02 – smb_proc_readX malicious data offset information leak:

Affected Kernels: 2.4

When receiving the answer to a readX request the Linux 2.4 kernel does not properly bounds check the supplied data offset. The check in place can fail because of a signedness issue. This means that a local attacker can leak kernel memory simply by issuing the read syscall on a smb filesystem when the connected server returns a data offset from outside the packet. This can of course also lead to a kernel crash when unallocated memory is accessed.

03 – smb_receive_trans2 defragmentation overflow:

Affected Kernels: 2.4

At the end of the TRANS2 defragmentation process the complete packet is moved to another place if a certain condition is true. In combination with [07] and the fact that the counters are not bounds checked before copying the data this can result in a kernel memory overflow.

04 – smb_proc_readX_data malicious data offset DOS:

Affected Kernels: 2.6

The server supplied data offset is decremented by the header size and then used as offset within the packet. While the supplied offset is checked against an upper bound it may have underflowed and therefore point outside the allocated memory. Any access to that memory could result in a crash.

05 – smb_receive_trans2 malicious parm/data offset info leak/DOS:

Affected Kernels: 2.4, 2.6

Both versions of the kernel do not properly bounds check the server supplied packet based offset of the parameters/data sent. This results in smbfs copying data from memory outside the received smb fragment into the

Securiteam: [UNIX] Linux 2.x smbfs Multiple Remote Vulnerabilities

receiving buffer. This can leak kernel memory to the calling function or result in a DOS because of accesses to unallocated memory.

06 – smb_recv_trans2 missing fragment information leak:

Affected Kernels: 2.4, 2.6

The defragmentation process of TRANS2 SMB packets does not properly initialize the receiving buffer. An attacker may f.e. send several thousand times the first byte of a packet until the received data count reaches the expected total and so leaks the rest of the uninitialized receiving buffer to the calling function.

07 – smb_recv_trans2 fragment resending leads to invalid counters:

Affected Kernels: 2.4, 2.6

The defragmentation termination condition is that at least the expected parameter count and at least the expected data count is reached. By using the fragment resending technique an attacker can increase one of those counters to an arbitrary high value.

Disclosure Timeline:

- 25. Sep 2004 Made initial contact with the Linux Developers
- 27. Sep 2004 Contacted vendor-sec about this issue
- 22. Oct 2004 Sent the 2nd round of smbfs vulnerabilities to both parties
- 27. Oct 2004 Sent final patchset for 2.4 and 2.6 kernel to the developers
- 11. Nov 2004 Linux 2.4.28-rc3 containing the final patchset was made available by the developers
- 17. Nov 2004 Linux 2.4.28 released
- 17. Nov 2004 Public Disclosure

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0883>>

CAN-2004-0883

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0949>>

CAN-2004-0949

ADDITIONAL INFORMATION

The information has been provided by <<mailto:s.esser@ematters.de>> Stefan Esser.

The original article can be found at:

<<http://security.e-matters.de/advisories/142004.html?SID=9452714072161c5f25d7312c0d23c30b>>

<http://security.e-matters.de/advisories/142004.html?SID=9452714072161c5f25d7312c0d23c30b>

=====

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

Securiteam: [UNIX] Linux 2.x smbfs Multiple Remote Vulnerabilities

=====
=====

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.