

# [UNIX] Samba "send\_mailslot()" Buffer Overflow Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-12/msg00024.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 11 Dec 2007 14:46:20 +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 "send\_mailslot()" Buffer Overflow Vulnerability

---

## SUMMARY

<<http://www.samba.org/>> Samba is "an Open Source/Free Software suite that has, since 1992, provided file and print services to all manner of SMB/CIFS clients, including the numerous versions of Microsoft Windows operating systems. Samba is freely available under the GNU General Public License". Secunia Research has discovered a vulnerability in Samba, which can be exploited by malicious people to compromise a vulnerable system.

## DETAILS

Vulnerable Systems:

\* Samba version 3.0.27a

The vulnerability is caused due to a boundary error within the "send\_mailslot()" function. This can be exploited to cause a stack-based buffer overflow with zero bytes via a specially crafted "SAMLOGON" domain logon packet containing a username string placed at an odd offset followed by an overly long GETDC string.

Successful exploitation allows execution of arbitrary code, but requires

[UNIX] Samba "send\_mailslot()" Buffer Overflow Vulnerability

that the "domain logons" option is enabled.

Time Table:

- 22/11/2007 – Vendor notified.
- 22/11/2007 – vendor–sec notified.
- 23/11/2007 – Vendor response.
- 10/12/2007 – Public disclosure.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6015>>  
 CVE-2007-6015

ADDITIONAL INFORMATION

The information has been provided by Secunia Research.

The original article can be found at:

<[http://secunia.com/secunia\\_research/2007-99/](http://secunia.com/secunia_research/2007-99/)>  
[http://secunia.com/secunia\\_research/2007-99/](http://secunia.com/secunia_research/2007-99/)

=====

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@xxxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====  
=====

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.