

# [VulnWatch] iDefense Security Advisory 05.14.07: Samba SAMR Change Password Remote Command Injection Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2007-05/msg00013.html>

---

- *From:* iDefense Labs <[labs-no-reply@xxxxxxxxxxxxx](mailto:labs-no-reply@xxxxxxxxxxxxx)>
  - *Date:* Mon, 14 May 2007 15:19:54 -0400
- 

Samba SAMR Change Password Remote Command Injection Vulnerability

iDefense Security Advisory 05.14.07  
<http://labs.iddefense.com/intelligence/vulnerabilities/>  
May 14, 2007

## I. BACKGROUND

Samba is a Unix server application used to implement Windows file sharing and domain controlling functionality. SAMR is the named pipe used to access the SAM, security accounts manager, database. This database stores login credentials on NT based systems. More information can be found at the following URL.

<http://samba.org/samba/>

## II. DESCRIPTION

Remote exploitation of a command injection vulnerability within Samba Project's Samba could allow an attacker to execute arbitrary code with nobody privileges.

The vulnerability exists within the code responsible for updating a user's password in the SAM database. Unfiltered user input is passed to "/bin/sh". This allows an attacker to execute arbitrary shell commands with the privileges of the nobody user.

## III. ANALYSIS

Successful exploitation of this vulnerability allows an attacker to run arbitrary shell commands with the privileges of the nobody user.

An important mitigating factor is that this vulnerability occurs within a non-default configuration of Samba. Specifically, the 'username map script' option must be defined in the smb.conf file.

Valid credentials are not needed to exploit this vulnerability. In order to successfully change a password, it is necessary to provide the original password. However, the vulnerability can still be triggered regardless of whether or not the change password attempt fails.

#### IV. DETECTION

iDefense has confirmed the existence of this vulnerability in Samba version 3.0.24. Previous versions of Samba release 3 may be vulnerable. Release version 2 and below did not have this feature.

#### V. WORKAROUND

Removing the 'username map script' option from the smb.conf file will prevent this vulnerability from being triggered.

#### VI. VENDOR RESPONSE

Samba has released version 3.0.25 as well as a patch for version 3.0.24 to address this issue. More information can be found in their announcement at the following URL.

<http://samba.org/samba/security/CVE-2007-2447.html>

#### VII. CVE INFORMATION

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2007-2447 to this issue. This is a candidate for inclusion in the CVE list (<http://cve.mitre.org/>), which standardizes names for security problems.

#### VIII. DISCLOSURE TIMELINE

05/07/2007 Initial vendor notification  
05/07/2007 Initial vendor response  
05/14/2007 Coordinated public disclosure

#### IX. CREDIT

The discoverer of this vulnerability wishes to remain anonymous.

Get paid for vulnerability research  
<http://labs.ndefense.com/methodology/vulnerability/vcp.php>

Free tools, research and upcoming events  
<http://labs.ndefense.com/>

#### X. LEGAL NOTICES

Copyright © 2007 iDefense, Inc.

Permission is granted for the redistribution of this alert electronically. It may not be edited in any way without the express written consent of iDefense. If you wish to reprint the whole or any part of this alert in any other medium other than electronically, please e-mail [customerservice@xxxxxxxxxxxx](mailto:customerservice@xxxxxxxxxxxx) for permission.

Disclaimer: The information in the advisory is believed to be accurate at the time of publishing based on currently available information. Use of the information constitutes acceptance for use in an AS IS condition. There are no warranties with regard to this information. Neither the author nor the publisher accepts any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.