

# SSRT3509 Potential Security Vulnerability in CIFS/9000 Server

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.misc/2003-03/0375.html>

---

**From:** Security Alert ([secure@cup.hp.com](mailto:secure@cup.hp.com))

**Date:** 03/18/03

From: [secure@cup.hp.com](mailto:secure@cup.hp.com) (Security Alert)

Date: Tue, 18 Mar 2003 15:23:17 GMT

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

---

Source: HEWLETT-PACKARD COMPANY  
SECURITY BULLETIN: HPSBUX0303-251  
Originally issued: 18 March 2003  
SSRT3509 Potential Security Vulnerability in CIFS/9000 Server

---

NOTICE: There are no restrictions for distribution of this Bulletin provided that it remains complete and intact.

The information in the following Security Bulletin should be acted upon as soon as possible. Hewlett-Packard Company will not be liable for any consequences to any customer resulting from customer's failure to fully implement instructions in this Security Bulletin as soon as possible.

---

**PROBLEM:** CIFS/9000 Server is potentially vulnerable to altered SMB/CIFS network messages.

**IMPACT:** Potential remote root access.

**PLATFORM:** All HP9000 servers running CIFS/9000 Server versions up to A.01.09.01 on HP-UX 11.0, 11.11(11i), and 11.22

**SOLUTION:** HP-UX 11.0/11.11

Download and install the smbd.11.00 file containing the fix. This file must be manually installed on the CIFS Server version A.01.09.01.

HP-UX 11.22

The CIFS Server must be disabled until the new

comp.security.misc: SSRT3509 Potential Security Vulnerability in CIFS/9000 Server

CIFS/9000 Server version A.01.09.02 is available on  
software.hp.com

MANUAL ACTIONS: Yes – NonUpdate

HP-UX 11.0/11.11  
Install the smbd.11.00 file.

HP-UX 11.22  
Disable the CIFS/9000 Server.

AVAILABILITY: The temporary fix, smbd.11.00, is available now.  
This bulletin will be revised when web upgrades  
are available.

---

A. Background

Note: The following are not vulnerable:

HP OpenVMS  
HP NonStop Servers  
HP Secure Web Servers for HP Tru64 UNIX  
HP Secure Web Servers for HP Tru64 OpenVMS

As further information becomes available HP  
will provide notice of the availability of any  
additional Samba updates through standard security  
bulletin announcements and information will be  
available from your normal HP Services support channel.

CIFS Server version A.01.09.01 and prior may allow modified  
SMB/CIFS messages to cause smbd to overwrite portions of its  
own process address space. This could potentially be  
exploited to gain root access remotely.

The latest version of CIFS Server adds checks for proper  
SMB/CIFS messages to prevent invalid smbd memory accesses.

The Samba team has provided a note describing ways to  
limit exposure to this vulnerability and future potential  
vulnerabilities. Please refer to Section E below.

B. Recommended solution

If /opt/samba/bin/smbd is present on a system the following  
instructions should be followed.

HP-UX 11.0/11.11

=====

Update to version A.01.09.01 if running earlier versions of  
CIFS Server (available on software.hp.com). Then download

and install the fixed smbd as detailed below.

When available on software.hp.com, install the complete CIFS Server 2.2d package (version A.01.09.02) to update the entire product.

Instructions for installing the fixed smbd:

1. Update to CIFS Server version A.01.09.01 if necessary.  
The CIFS Server is available on software.hp.com

2. Download new smbd.11.00.gz binary file:

System: hprc.external.hp.com (192.170.19.51)

Login: samba

Password: samba

FTP Access: <ftp://samba:samba@hprc.external.hp.com/>

or: <ftp://samba:samba@192.170.19.51/>

or: ftp hprc.external.hp.com

Note: There is an ftp defect in IE5 that may result in a browser hang. To work around this:

– Select Tools –> Internet Options –> Advanced

– Un-check the option:

[ ] Enable folder view for FTP sites

3. Unpack the file with gunzip and verify the cksum or the md5 sum:

cksum:

3908130721 2555904 smbd.11.00

MD5 (smbd.11.00) = 24eb08b309ea60c6d48e27fc66b5f8

Note: If you wish to verify the md5 sum and you do not have a copy of md5, please refer to:

HPSBUX9408-016

Patch sums and the MD5 program

Note: Using your itrc account security bulletins can be found here:

<http://itrc.hp.com/cki/bin/doc.pl/screen=ckiSecurityBulletin>

4. Replace current smbd file with new version:

Back up the original smbd file : /opt/samba/bin/smbd

Stop CIFS/9000 Server if it is running.

Copy the downloaded smbd.11.00 to /opt/samba/bin/smbd

Note: smbd.11.00 is for both HP-UX 11.00 and

HP-UX 11.11 (11i).

Restart CIFS/9000 Server if it had been running.

HP-UX 11.22

=====

Disable the CIFS/9000 Server.

C. To subscribe to automatically receive future NEW HP Security Bulletins from the HP IT Resource Center via electronic mail, do the following:

Use your browser to get to the HP IT Resource Center page at:

<http://itrc.hp.com>

Use the 'Login' tab at the left side of the screen to login using your ID and password. Use your existing login or the "Register" button at the left to create a login, in order to gain access to many areas of the ITRC. Remember to save the User ID assigned to you, and your password.

In the left most frame select "Maintenance and Support".

Under the "Notifications" section (near the bottom of the page), select "Support Information Digests".

To –subscribe– to future HP Security Bulletins or other Technical Digests, click the check box (in the left column) for the appropriate digest and then click the "Update Subscriptions" button at the bottom of the page.

or

To –review– bulletins already released, select the link (in the middle column) for the appropriate digest.

NOTE: Using your itrc account security bulletins can be found here:

<http://itrc.hp.com/cki/bin/doc.pl/screen=ckiSecurityBulletin>

To –gain access– to the Security Patch Matrix, select the link for "The Security Bulletins Archive". (near the bottom of the page) Once in the archive the third link is to the current Security Patch Matrix. Updated daily, this matrix categorizes security patches by platform/OS release, and by bulletin topic. Security Patch Check completely automates the process of reviewing the patch matrix for 11.XX systems. Please note that installing the patches listed in the Security Patch Matrix will completely

implement a security bulletin \_only\_ if the MANUAL ACTIONS field specifies "No."

The Security Patch Check tool can verify that a security bulletin has been implemented on HP-UX 11.XX systems providing that the fix is completely implemented in a patch with no manual actions required. The Security Patch Check tool cannot verify fixes implemented via a product upgrade.

For information on the Security Patch Check tool, see:  
[http://www.software.hp.com/cgi-bin/swdepot\\_parser.cgi/cgi/displayProductInfo.pl?productNumber=B6834AA](http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=B6834AA)

The security patch matrix is also available via anonymous ftp:

[ftp://ftp.itrc.hp.com/export/patches/hp-ux\\_patch\\_matrix/](ftp://ftp.itrc.hp.com/export/patches/hp-ux_patch_matrix/)

On the "Support Information Digest Main" page:  
click on the "HP Security Bulletin Archive".

The PGP key used to sign this bulletin is available from several PGP Public Key servers. The key identification information is:

2D2A7D59  
HP Security Response Team (Security Bulletin signing only)  
<[security-alert@hp.com](mailto:security-alert@hp.com)>  
Fingerprint =  
6002 6019 BFC1 BC62 F079 862E E01F 3AFC 2D2A 7D59

If you have problems locating the key please write to [security-alert@hp.com](mailto:security-alert@hp.com). Please note that this key is for signing bulletins only and is not the key returned by sending 'get key' to [security-alert@hp.com](mailto:security-alert@hp.com).

D. To report new security vulnerabilities, send email to

[security-alert@hp.com](mailto:security-alert@hp.com)

Please encrypt any exploit information using the [security-alert](mailto:security-alert@hp.com) PGP key, available from your local key server, or by sending a message with a `-subject-` (not body) of 'get key' (no quotes) to [security-alert@hp.com](mailto:security-alert@hp.com).

E. Samba Team notes on protecting an unpatched Samba server

\*\*\*\*\*

Protecting an unpatched Samba server

\*\*\*\*\*

This is a note on how to provide your Samba server some protection against the potential vulnerability even if you are unable to upgrade to the fixed version immediately. Even if you do upgrade these suggestions provide additional levels of protection against possible future vulnerabilities.

#### Using host based protection

---

In many installations of Samba the greatest threat comes from outside the immediate network. By default Samba will accept connections from any host.

One of the simplest fixes in this case is to use the 'hosts allow' and 'hosts deny' options in the Samba smb.conf configuration file to only allow access to your server from a specific range of hosts. An example might be:

```
hosts allow = 127.0.0.1 192.168.2.0/24 192.168.3.0/24
hosts deny = 0.0.0.0/0
```

The above will only allow SMB connections from 'localhost' (your own computer) and from the two private networks 192.168.2 and 192.168.3. All other connections will be refused connections as soon as the client sends its first packet. The refusal will be marked as a 'not listening on called name' error.

#### Using interface protection

---

By default Samba will accept connections on any network interface that it finds on your system. That means if you have a ISDN line or a PPP connection to the Internet then Samba will accept connections on those links. This may not be what you want.

You can change this behavior using options like the following:

```
interfaces = lan* lo0
bind interfaces only = yes
```

that tells Samba to only listen for connections on interfaces with a name starting with 'lan' such as lan0, lan1, plus on the loopback interface called 'lo0'. The name you will need to use depends on what OS you are using. The example above uses the common name for ethernet adapters on HP-UX.

If you use the above and someone tries to make a SMB connection to your host over a PPP interface called 'ppp0', they will get a TCP connection refused reply. In that case no Samba code is run at all as the operating system has been told not to pass connections from that interface to any process.

#### Using a firewall

---

Many people use a firewall to deny access to services that they do not want exposed outside their network. This can be a very good idea, although the methods above should also be used in case the firewall is not active for some reason.

If you are setting up a firewall then you need to know what TCP and UDP ports to allow and block. Samba uses the following:

- UDP/137 – used by nmbd
- UDP/138 – used by nmbd
- TCP/139 – used by smb
- TCP/445 – used by smb

The last one is important as many older firewall setups may not be aware of it, given that this port was only added to the protocol in recent years.

#### Using a IPC\$ share deny

---

If the above methods are not suitable, then you could also place a more specific deny on the IPC\$ share that is used in the vulnerability reported in this bulletin. This allows you to offer access to other shares while denying access to IPC\$ from potentially untrustworthy hosts.

To do that you could use:

```
[ipc$]
hosts allow = 192.168.115.0/24 127.0.0.1
hosts deny = 0.0.0.0/0
```

this would tell Samba that IPC\$ connections are not allowed from anywhere but the two listed places (localhost and a local subnet). Connections to other shares would still be allowed. As the IPC\$ share is the only share that is always accessible anonymously this provides some level of protection against attackers that do not know a username/password for your host.

comp.security.misc: SSRT3509 Potential Security Vulnerability in CIFS/9000 Server

If you use this method then clients will be given an 'access denied' reply when they try to access the IPC\$ share. That means that those clients will not be able to browse shares, and may also be unable to access some other resources.

---

(c)Copyright 2003 Hewlett-Packard Company  
Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein. The information in this document is subject to change without notice.  
Hewlett-Packard Company and the names of HP products referenced herein are trademarks and/or service marks of Hewlett-Packard Company. Other product and company names mentioned herein may be trademarks and/or service marks of their respective owners.

---

-----BEGIN PGP SIGNATURE-----

Version: PGP Personal Security 7.0.3

iQA/AwUBPnY+eeAfOvwtKn1ZEqKCCQCg2CsOpVPI/xdTDzqH/Vd/dgYNsG4AoM4k  
2kVYyUp9YZ7JJDbL9zRi0ka8  
=B0a7

-----END PGP SIGNATURE-----

--  
Yours truly,  
HP S/W Security Team  
WTEC Cupertino, California  
Return-Path: [secure@cup.hp.com](mailto:secure@cup.hp.com)  
Reply-to: [security-alert@hp.com](mailto:security-alert@hp.com)