

# [Full-Disclosure] R: Full-Disclosure Digest, Vol 3, Issue 42

**Source:** <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-02/0660.html>

---

**From:** Tiziano Radice (*t.radice\_at\_wssitalia.it*)

**Date:** 02/22/05

To: <full-disclosure@lists.netsys.com>

Date: Tue, 22 Feb 2005 10:32:30 +0100

Help: please remove me from your mail list

-----Messaggio originale-----

Da: full-disclosure-bounces@lists.netsys.com

[mailto:full-disclosure-bounces@lists.netsys.com] Per conto di

full-disclosure-request@lists.netsys.com

Inviato: martedì 22 febbraio 2005 8.17

A: full-disclosure@lists.netsys.com

Oggetto: Full-Disclosure Digest, Vol 3, Issue 42

Send Full-Disclosure mailing list submissions to  
full-disclosure@lists.netsys.com

To subscribe or unsubscribe via the World Wide Web, visit  
<https://lists.netsys.com/mailman/listinfo/full-disclosure>  
or, via email, send a message with subject or body 'help' to  
full-disclosure-request@lists.netsys.com

You can reach the person managing the list at  
full-disclosure-owner@lists.netsys.com

When replying, please edit your Subject line so it is more specific  
than "Re: Contents of Full-Disclosure digest..."

Today's Topics:

1. Shadow Crew back in business (n3td3v)
2. iDEFENSE Security Advisory 02.21.05: Multiple PuTTY SFTP Client Packet Parsing Integer Overflow Vulnerabilities (idlabs-advisories@idefense.com)
3. SD Server 4.0.70 Directory Traversal Bug (CorryL)
4. iDEFENSE Security Advisory 02.21.05: Multiple Unix/Linux Vendor cURL/libcURL NTLM Authentication Buffer Overflow Vulnerability (idlabs-advisories@idefense.com)
5. iDEFENSE Security Advisory 02.21.05: Multiple Unix/Linux

- Vendor cURL/libcURL Kerberos Authentication Buffer Overflow  
Vulnerability (idlabs-advisories@idefense.com)
6. [ GLSA 200502-28 ] PuTTY: Remote code execution (Luke Macken)
  7. [gentoo-announce] [ GLSA 200502-28 ] PuTTY: Remote code execution (Luke Macken)
  8. Awake a modem with AT commands (action09)
  9. Sourceforge security contact to the white courtesy phone please. (J.A. Terranson)
  10. Delivery by mail (Rizwanalikhhan)
  11. Re: Arkeia Network Backup Client Remote Access (H D Moore)
  12. phpBB Fixed full path disclosure in username handling – 2.0.11 (Aaron Horst)
  13. Registration is accepted (Rizwanalikhhan)
- 

Message: 1

Date: Mon, 21 Feb 2005 17:47:40 +0000

From: n3td3v <xploitable@gmail.com>

Subject: [Full-Disclosure] Shadow Crew back in business

To: full-disclosure@lists.netsys.com

Message-ID: <4b6ee93105022109476c88ac53@mail.gmail.com>

Content-Type: text/plain; charset=US-ASCII

The Shadow Crew who are under investigation and the American Secret Service replaced the homepage of, with a federal notice, is back in business on a new domain.

Seen today on the popular chat service Yahoo! Chat, spamming its advert as the alias "fire\_p0w3r"

An example of the spam is below:

fire\_p0w3r: Want CC ? Credit Cards and Carding Related Subjects ,  
Cyberspace , Novelty Identification, Documents and other Related  
Subjects , Tutorials and How-To's , Non-business related talks ,  
Scumbags & Rippers , Hardware and Other Related Subjects , Vendor's  
products & services , Request Review , Auction Forum , Feedbacks ,  
STRICTLY BUSINESS , Then Come And Register At [www.Shadow-Crew.net](http://www.Shadow-Crew.net) NOW  
!

Hopefully the American Secret Service will shut this site down like they did with the other.

I advise Yahoo! to suspend the account fire\_p0w3r, while keeping the connection information for when the American Secret Service come to get it from you.

Thanks, n3td3v

My list is located at <http://groups-beta.google.com/group/n3td3v> if you want off-list contact.

Hi to Yahoo! Security Team and the American Secret Service, n3td3v is always happy to provide intelligence to take away silly groups like Shadow Crew.

-----  
Message: 2

Date: Mon, 21 Feb 2005 13:02:24 -0500

From: idlabs-advisories@idefense.com

Subject: [Full-Disclosure] iDEFENSE Security Advisory 02.21.05:  
Multiple PuTTY SFTP Client Packet Parsing Integer Overflow  
Vulnerabilities

To: <idlabs-advisories@idefense.com>

Message-ID:

<FB24803D1DF2A34FA59FC157B77C970503E24608@idserv04.idef.com>

Content-Type: text/plain; charset="iso-8859-1"

Multiple PuTTY SFTP Client Packet Parsing Integer Overflow  
Vulnerabilities

[www.idefense.com/application/poi/display?id=201&type=vulnerabilities](http://www.idefense.com/application/poi/display?id=201&type=vulnerabilities)  
February 21, 2005

## I. BACKGROUND

PuTTY is a free implementation of Telnet and SSH for Win32 and Unix platforms, along with an xterm terminal emulator.

More information is available on the vendor's website:

<http://www.chiark.greenend.org.uk/~sgtatham/putty/>

## II. DESCRIPTION

Remote exploitation of multiple integer overflow vulnerabilities in Simon Tatham's PuTTY can allow attackers to execute arbitrary code.

The first vulnerability specifically exists due to insufficient validation of user-supplied data passed to a memcpy function. The PuTTY sftp implementation allows attackers to supply arbitrary values for the stored length of the string in the packet. This may be observed in the sftp\_pkt\_getstring() function from sftp.c in PuTTY source code:

```
static void sftp_pkt_getstring(struct sftp_packet *pkt,  
                             char **p, int *length)  
{  
    *p = NULL;  
    if (pkt->length - pkt->savedpos < 4)
```

```

    return;
/* length value is taken from user-supplied data */
*length = GET_32BIT(pkt->data + pkt->savedpos);
pkt->savedpos += 4;
/* this check will be passed if length < 0 */
if (pkt->length - pkt->savedpos < *length)
    return;
*p = pkt->data + pkt->savedpos;
pkt->savedpos += *length;
}

```

This function is called from `fxp_open_recv()` and passes the returned string pointer and string length to the `mkstr()` function:

```

struct fxp_handle *fxp_open_recv(struct sftp_packet *pktin,
    struct sftp_request *req)
{
    ...
/* sftp_pkt_getstring call with controlled len value */
sftp_pkt_getstring(pktin, &hstring, &len);
    ...
    handle = snwn(struct fxp_handle);
/* heap corruption will occur if len == -1 */
    handle->hstring = mkstr(hstring, len);
    handle->hlen = len;
    sftp_pkt_free(pktin);
    return handle;
    ...
}

```

If `length` is passed as `-1`, a `malloc(0)` will occur when the `snwn()` macro is called:

```

static char *mkstr(char *s, int len)
{
/* malloc(0) if len == -1 */
    char *p = snwn(len + 1, char);
/* user controlled heap corruption */
    memcpy(p, s, len);
    p[len] = '\0';
    return p;
}

```

Finally, when the `memcpy` function is called heap corruption will occur leading to potential code execution.

The second vulnerability specifically exists due to insufficient validation of user-supplied data passed to a `malloc` function. This may be observed in the `fxp_readdir_recv()` function from PuTTY source code:

```

struct fxp_names *fxp_readdir_recv(struct sftp_packet *pktin,
                                   struct sftp_request *req) {
    /* 32 bit value from packet */
    ret->nnames = sftp_pkt_getuint32(pktin);
    /*
     * The integer overflow occurs when ret->nnames is referenced
     * the snewn macro calls malloc() wrapper
     * #define snewn(n, type) ((type *)smalloc((n)*sizeof(type)))
     */
    ret->names = snewn(ret->nnames, struct fxp_name);
    for (i = 0; i < ret->nnames; i++) {
        char *str;
        int len;
        sftp_pkt_getstring(pktin, &str, &len);
        /* pointer to arbitrary data from packet */
        ret->names[i].filename = mkstr(str, len);
        sftp_pkt_getstring(pktin, &str, &len);
        /* pointer to arbitrary data from packet */
        ret->names[i].longname = mkstr(str, len);
        /* pointer to arbitrary data from packet */
        ret->names[i].attrs = sftp_pkt_getattrs(pktin);
    }
}

```

This function is called from `scp_get_sink_action()` in `scp.c` and `sftp_cmd_ls()` in `sftp.c` and can lead to remote code execution via heap corruption. Sample debugger output of heap corruption is shown below:

```

psftp> ls
Listing directory /home/test

```

```

Program received signal SIGSEGV, Segmentation fault.
0x4009173c in memcpy () from /lib/libc.so.6
(gdb) bt
#0 0x4009173c in memcpy () from /lib/libc.so.6
#1 0x0805675f in mkstr (s=0x4e20 <Address 0x4e20 out of bounds>, len=0)
#2 0x0805748e in fxp_readdir_recv (pktin=0x809bc10, req=0x4e20)
#3 0x0804f7b8 in sftp_cmd_ls (cmd=0x4e20) at ../psftp.c:251
#4 0x08051955 in do_sftp (mode=0, modeflags=0, batchfile=0x0)
#5 0x080525f8 in psftp_main (argc=4, argv=0xbffff494)
#6 0x08080500 in main (argc=20000, argv=0x4e20)
(gdb) up 2
#2 0x0805748e in fxp_readdir_recv (pktin=0x809bc10, req=0x4e20)
952 ret->names[i].filename = mkstr(str, len);
(gdb) x/8x *(int)pktin
0x80acc58: 0x01000068 0x66666600 0x00000067 0x42424208
0x80acc68: 0x42424242 0x00000042 0x44444408 0x44444444
(gdb) print (struct sftp_packet)pktin
$2 = {data = 0x809bc10 "XL\n\bYF", length = 134885120,
maxlen = -1073744968, savedpos = 134551097, type = 134885088}

```

### III. ANALYSIS

Successful exploitation allows remote attackers to execute arbitrary code under the privileges of the user running PuTTY. The client must be directed to connect to a malicious server in order to trigger the vulnerability. It should be noted that this vulnerability may affect applications which use PuTTY source code or binaries as a SSH protocol backend. An example of one such product would be WinSCP3, a popular graphical sftp/scp application for Windows.

#### IV. DETECTION

iDEFENSE has confirmed that PuTTY 0.56 is vulnerable. It is suspected that earlier versions are also vulnerable.

The following vendors distribute susceptible PuTTY packages within their respective operating system distributions:

\* FreeBSD Project:

FreeBSD 4.9, 4.10, 5.0, 5.1 and 5.2.1

\* Gentoo Foundation Inc.:

Gentoo Linux 1.1a, 1.2, 1.4, 2004.0, 2004.1 and 2004.2

#### V. WORKAROUND

Use an alternate SSH client to connect to untrusted hosts until the vendor releases a patch.

#### VI. VENDOR RESPONSE

Vendor advisories for these issues are available at:

<http://www.chiark.greenend.org.uk/~sgtatham/putty/wishlist/vuln-sftp-string.html>

<http://www.chiark.greenend.org.uk/~sgtatham/putty/wishlist/vuln-sftp-readdir.html>

#### VII. CVE INFORMATION

The Common Vulnerabilities and Exposures (CVE) project has assigned the names CAN-2005-0467 to these issues. This is a candidate for inclusion in the CVE list (<http://cve.mitre.org>), which standardizes names for security problems.

#### VIII. DISCLOSURE TIMELINE

02/18/2005 Initial vendor notification

02/19/2005 Initial vendor response

02/21/2005 Public disclosure

#### IX. CREDIT

Gagl Delalleau credited with this discovery.

Get paid for vulnerability research  
<http://www.odefense.com/poi/teams/vcp.jsp>

## X. LEGAL NOTICES

Copyright ) 2005 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 email [customerservice@odefense.com](mailto:customerservice@odefense.com) 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.

-----  
Message: 3  
Date: Mon, 21 Feb 2005 20:41:49 +0100  
From: "CorryL" <[corryl@sitoverde.com](mailto:corryl@sitoverde.com)>  
Subject: [Full-Disclosure] SD Server 4.0.70 Directory Traversal Bug  
To: <[full-disclosure@lists.netsys.com](mailto:full-disclosure@lists.netsys.com)>  
Cc: [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)  
Message-ID: <00d001c5184d\$63772bf0\$0100a8c0@server>  
Content-Type: text/plain; charset="iso-8859-1"

...:x0n3-h4ck Italian Security Team:..

/\*Advisories\*\

\*/

Application: SD Server

Url Vendor: <http://www.gdsoftware.dk/>

Version: <= 4.0.70

Platforms: Windows

Bug: Directory Traversal

Exploitation: Remote

Author: CorryL

Email Author: corryl80@gmail.com

Url Author: www.x0n3-h4ck.org

\*\

{Description}

The SD Server is a easy http server, A remote user can obtain files on the system that are located outside of the web document directory.

{Bug}

<http://victimhost/../../../../windows/repair/sam>

A remote user succeeds to read the file sam of the system where to be in execution SD Server.

{Vendor Status}

20/02/2005 Vendor notification

20/02/2005 Vendor response

21/02/2005 Vendor Fix the Bug

{Fix}

In version 4.0.0.72

[http://www.gdssoftware.dk/dl\\_file.asp?link=SDServer 4.0.0.72.zip](http://www.gdssoftware.dk/dl_file.asp?link=SDServer 4.0.0.72.zip)

CorryL  
corryl80@gmail.com  
www.x0n3-h4ck.org  
Italian Security Team

---

www.seekstat.it is your web stat

---

Message: 4

Date: Mon, 21 Feb 2005 15:28:41 -0500

From: idlabs-advisories@idefense.com

Subject: [Full-Disclosure] iDEFENSE Security Advisory 02.21.05:  
Multiple Unix/Linux Vendor cURL/libcURL NTLM  
Authentication Buffer

## Overflow Vulnerability

To: <idlabs-advisories@idefense.com>

Message-ID:

<FB24803D1DF2A34FA59FC157B77C970503E24617@idserv04.idef.com>

Content-Type: text/plain; charset="us-ascii"

## Multiple Unix/Linux Vendor cURL/libcURL NTLM Authentication Buffer Overflow Vulnerability

iDEFENSE Security Advisory 02.21.05:

[www.idefense.com/application/poi/display?id=202&type=vulnerabilities](http://www.idefense.com/application/poi/display?id=202&type=vulnerabilities)

February 21, 2005

### I. BACKGROUND

cURL is a command line tool for transferring files with URL syntax, supporting FTP, FTPS, HTTP, HTTPS, GOPHER, TELNET, DICT, FILE and LDAP. More information about cURL and libcURL is available from:

<http://curl.haxx.se/>

### II. DESCRIPTION

Remote exploitation of a stack-based buffer overflow in various Unix / Linux vendors implementations of cURL could allow for arbitrary code execution on the targeted host.

An exploitable stack-based buffer overflow condition exists when using NT Lan Manager (NTLM) authentication. The problem specifically exists within `Curl_input_ntlm()` defined in `lib/http_ntlm.c`. Within this function an unsigned stack-based character array of size 256, `buffer[]`, is passed to the `Curl_base64_decode()` routine defined in `lib/base64.c` as can be seen here:

```
size_t size = Curl_base64_decode(header, (char *)buffer);
```

The `Curl_base64_decode()` routine relies on the calling function to validate the decoded length. This function base64 decodes and copies data directly from the HTTP reply of a server to the destination buffer, in this case `buffer[]`. An attacker can construct a long base64 encoded malicious payload that upon decoding will overflow the 256 byte static buffer and overwrite the saved EIP. This in turn can lead to arbitrary code execution.

### III. ANALYSIS

Successful exploitation allows remote attackers to execute arbitrary code under the privileges of the target user. Exploitation requires that an attacker either coerce or force a target to connect to a malicious server using NTLM authentication.

#### IV. DETECTION

iDEFENSE has confirmed the existence of this vulnerability in cURL version 7.12.1. It is suspected that prior versions are affected as well.

Any application built using a vulnerable version libcurl will also be affected.

#### V. WORKAROUND

Replace the static buffer allocation on line 106 in lib/http\_ntlm.c:

```
unsigned char buffer[256];
```

With a dynamic buffer allocation:

```
unsigned char *buffer = (unsigned char *)malloc(strlen(header));
```

and recompile cURL.

#### VI. VENDOR RESPONSE

No vendor response received.

#### VII. CVE INFORMATION

A Mitre Corp. Common Vulnerabilities and Exposures (CVE) number has not been assigned yet.

#### VIII. DISCLOSURE TIMELINE

12/21/2004 Initial vendor notification – No response  
02/10/2005 Secondary vendor notification – No response  
02/21/2005 Public disclosure

#### IX. CREDIT

infamous41md[at]hotpop.com is credited with this discovery.

Get paid for vulnerability research  
<http://www.idefense.com/poi/teams/vcp.jsp>

#### X. LEGAL NOTICES

Copyright (c) 2005 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 email customerservice@idefense.com 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.

---

Message: 5

Date: Mon, 21 Feb 2005 15:28:42 -0500

From: idlabs-advisories@idefense.com

Subject: [Full-Disclosure] iDEFENSE Security Advisory 02.21.05:

Multiple Unix/Linux Vendor cURL/libcURL Kerberos

Authentication Buffer

Overflow Vulnerability

To: <idlabs-advisories@idefense.com>

Message-ID:

<FB24803D1DF2A34FA59FC157B77C970503E24618@idserv04.idef.com>

Content-Type: text/plain; charset="us-ascii"

Multiple Unix/Linux Vendor cURL/libcURL Kerberos Authentication Buffer  
Overflow Vulnerability

iDEFENSE Security Advisory 02.21.05:

[www.idefense.com/application/poi/display?id=203&type=vulnerabilities](http://www.idefense.com/application/poi/display?id=203&type=vulnerabilities)

February 21, 2005

## I. BACKGROUND

cURL is a command line tool for transferring files with URL syntax, supporting FTP, FTPS, HTTP, HTTPS, GOPHER, TELNET, DICT, FILE and LDAP. More information about cURL and libcURL is available from:

<http://curl.haxx.se/>

## II. DESCRIPTION

Remote exploitation of a stack-based buffer overflow in various Unix / Linux vendors' implementation of cURL could allow for arbitrary code execution on the targeted host.

An exploitable stack-based buffer overflow condition exists when using Kerberos authentication. The problem specifically exists within the functions `Curl_krb_kauth()` and `krb4_auth()` defined in `lib/krb4.c`. Within these functions a statically allocated stack-based buffer of size 1250, from struct `KTEXT_ST.dat`, is passed to the `Curl_base64_decode()` routine defined in `lib/base64.c` as can be seen here:

```
len = Curl_base64_decode(p, (char *)adat.dat);  
tmp = Curl_base64_decode(p, (char *)tkk.dat);
```

The Curl\_base64\_decode() routine relies on the calling function to validate the decoded length. This function base64 decodes and copies data directly from the HTTP reply of a server to the destination buffer, in this case buffer[]. An attacker can construct a long base64 encoded malicious payload that upon decoding will overflow the static buffer and overwrite the saved EIP. This in turn can lead to arbitrary code execution.

### III. ANALYSIS

Successful exploitation allows remote attackers to execute arbitrary code under the privileges of the target user. Exploitation requires that an attacker either coerce or force a target to connect to a malicious server using Kerberos authentication.

### IV. DETECTION

iDEFENSE has confirmed the existence of this vulnerability in cURL version 7.12.1. It is suspected that prior versions are affected as well.

Any application built using a vulnerable version libcurl will also be affected.

### V. WORKAROUND

Recompile cURL without Kerberos support if it is not needed.

### VI. VENDOR RESPONSE

No vendor response received.

### VII. CVE INFORMATION

A Mitre Corp. Common Vulnerabilities and Exposures (CVE) number has not been assigned yet.

### VIII. DISCLOSURE TIMELINE

12/23/2004 Initial vendor notification – No response  
02/10/2005 Secondary vendor notification – No response  
02/21/2005 Public disclosure

### IX. CREDIT

infamous41md[at]hotpop.com is credited with this discovery.

Get paid for vulnerability research  
<http://www.idefense.com/poi/teams/vcp.jsp>

## X. LEGAL NOTICES

Copyright (c) 2005 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 email [customerservice@idefense.com](mailto:customerservice@idefense.com) 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.

---

Message: 6  
Date: Mon, 21 Feb 2005 16:01:26 -0500  
From: Luke Macken <[lewk@gentoo.org](mailto:lewk@gentoo.org)>  
Subject: [Full-Disclosure] [ GLSA 200502-28 ] PuTTY: Remote code execution  
To: [gentoo-announce@gentoo.org](mailto:gentoo-announce@gentoo.org)  
Cc: [security-alerts@linuxsecurity.com](mailto:security-alerts@linuxsecurity.com), [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com),  
[full-disclosure@lists.netsys.com](mailto:full-disclosure@lists.netsys.com)  
Message-ID: <20050221210126.GA18728@tomserve.hsd1.ma.comcast.net>  
Content-Type: text/plain; charset="us-ascii"

---

Gentoo Linux Security Advisory GLSA 200502-28

---

<http://security.gentoo.org/>

---

Severity: Normal  
Title: PuTTY: Remote code execution  
Date: February 21, 2005  
Bugs: #82753  
ID: 200502-28

---

Synopsis

=====

PuTTY was found to contain vulnerabilities that can allow a malicious SFTP server to execute arbitrary code on unsuspecting PSCP and PSFTP clients.

#### Background

=====

PuTTY is a popular SSH client, PSCP is a secure copy implementation, and PSFTP is a SSH File Transfer Protocol client.

#### Affected packages

=====

-----  
Package / Vulnerable / Unaffected  
-----

1 net-misc/putty < 0.57 >= 0.57

#### Description

=====

Two vulnerabilities have been discovered in the PSCP and PSFTP clients, which can be triggered by the SFTP server itself. These issues are caused by the improper handling of the FXP\_READDIR response, along with other string fields.

#### Impact

=====

An attacker can setup a malicious SFTP server that would send these malformed responses to a client, potentially allowing the execution of arbitrary code on their system.

#### Workaround

=====

There is no known workaround at this time.

#### Resolution

=====

All PuTTY users should upgrade to the latest version:

```
# emerge --sync
# emerge --ask --oneshot --verbose ">=net-misc/putty-0.57"
```

#### References

=====

[ 1 ] PuTTY vulnerability vuln-sftp-readdir

<http://www.chiark.greenend.org.uk/~sgtatham/putty/wishlist/vuln-sftp-readdir.html>

[ 2 ] PuTTY vulnerability vuln-sftp-string

<http://www.chiark.greenend.org.uk/~sgtatham/putty/wishlist/vuln-sftp-string.html>

[ 3 ] CAN-2005-0467

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0467>

[ 4 ] iDEFENSE Advisory

<http://www.iddefense.com/application/poi/display?id=201&type=vulnerabilities>

#### Availability

=====

This GLSA and any updates to it are available for viewing at the Gentoo Security Website:

<http://security.gentoo.org/glsa/glsa-200502-28.xml>

#### Concerns?

=====

Security is a primary focus of Gentoo Linux and ensuring the confidentiality and security of our users machines is of utmost importance to us. Any security concerns should be addressed to [security@gentoo.org](mailto:security@gentoo.org) or alternatively, you may file a bug at <http://bugs.gentoo.org>.

#### License

=====

Copyright 2005 Gentoo Foundation, Inc; referenced text belongs to its owner(s).

The contents of this document are licensed under the Creative Commons – Attribution / Share Alike license.

<http://creativecommons.org/licenses/by-sa/2.0>

----- next part -----

A non-text attachment was scrubbed...

Name: not available

Type: application/pgp-signature

Size: 189 bytes

Desc: not available

Url :

<http://lists.netsys.com/pipermail/full-disclosure/attachments/20050221/0cd06bdd/attachment-0001.bin>

-----

Message: 7

Date: Mon, 21 Feb 2005 16:01:26 -0500

From: Luke Macken <lewk@gentoo.org>

Subject: [Full-Disclosure] [gentoo-announce] [ GLSA 200502-28 ] PuTTY:

Remote code execution

To: the\_eye@drei.at

Cc: security-alerts@linuxsecurity.com, bugtraq@securityfocus.com,  
full-disclosure@lists.netsys.com

Message-ID: <20050221210126.GA18728@tomservo.hsd1.ma.comcast.net>

Content-Type: text/plain; charset="us-ascii"

-----  
Gentoo Linux Security Advisory GLSA 200502-28  
-----

<http://security.gentoo.org/>  
-----

Severity: Normal

Title: PuTTY: Remote code execution

Date: February 21, 2005

Bugs: #82753

ID: 200502-28  
-----

Synopsis

=====

PuTTY was found to contain vulnerabilities that can allow a malicious SFTP server to execute arbitrary code on unsuspecting PSCP and PSFTP clients.

Background

=====

PuTTY is a popular SSH client, PSCP is a secure copy implementation, and PSFTP is a SSH File Transfer Protocol client.

Affected packages

=====

-----  
Package / Vulnerable / Unaffected  
-----

1 net-misc/putty < 0.57 >= 0.57

Description

=====

Two vulnerabilities have been discovered in the PSCP and PSFTP clients, which can be triggered by the SFTP server itself. These issues are

caused by the improper handling of the FXP\_READDIR response, along with other string fields.

#### Impact

=====

An attacker can setup a malicious SFTP server that would send these malformed responses to a client, potentially allowing the execution of arbitrary code on their system.

#### Workaround

=====

There is no known workaround at this time.

#### Resolution

=====

All PuTTY users should upgrade to the latest version:

```
# emerge --sync
# emerge --ask --oneshot --verbose ">=net-misc/putty-0.57"
```

#### References

=====

[ 1 ] PuTTY vulnerability vuln-sftp-readdir

<http://www.chiark.greenend.org.uk/~sgtatham/putty/wishlist/vuln-sftp-readdir.html>

[ 2 ] PuTTY vulnerability vuln-sftp-string

<http://www.chiark.greenend.org.uk/~sgtatham/putty/wishlist/vuln-sftp-string.html>

[ 3 ] CAN-2005-0467

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0467>

[ 4 ] iDEFENSE Advisory

<http://www.iddefense.com/application/poi/display?id=201&type=vulnerabilities>

#### Availability

=====

This GLSA and any updates to it are available for viewing at the Gentoo Security Website:

<http://security.gentoo.org/glsa/glsa-200502-28.xml>

#### Concerns?

=====

Security is a primary focus of Gentoo Linux and ensuring the confidentiality and security of our users machines is of utmost importance to us. Any security concerns should be addressed to [security@gentoo.org](mailto:security@gentoo.org) or alternatively, you may file a bug at <http://bugs.gentoo.org>.

License

=====

Copyright 2005 Gentoo Foundation, Inc; referenced text belongs to its owner(s).

The contents of this document are licensed under the Creative Commons – Attribution / Share Alike license.

<http://creativecommons.org/licenses/by-sa/2.0>

----- next part -----

A non-text attachment was scrubbed...

Name: not available

Type: application/pgp-signature

Size: 189 bytes

Desc: not available

Url :

<http://lists.netsys.com/pipermail/full-disclosure/attachments/20050221/0cd06bdd/attachment-0002.bin>

-----  
Message: 8

Date: Tue, 22 Feb 2005 00:17:08 +0100

From: action09 <action09@aimao.org>

Subject: [Full-Disclosure] Awake a modem with AT commands

To: full-disclosure@lists.netsys.com

Message-ID: <1109027828.5917.18.camel@workstation>

Content-Type: text/plain

Hi!

I'm looking for specially crafted Hayes AT commands to awake a computer ( behind a firewall, connected to an internal LAN , but --also-- connected to an external phone line ) .

The machine is a Windows 2K Pro, someone can help please ?

Is there a way to awake a dialup modem, have a shell on it after ? how ?

Thx a by advance dor any clue.

sorry for my bad english.

A-Xess

---

Message: 9  
Date: Mon, 21 Feb 2005 17:44:24 -0600 (CST)  
From: "J.A. Terranson" <measl@mfn.org>  
Subject: [Full-Disclosure] Sourceforge security contact to the white  
courtesy phone please.  
To: full-disclosure@lists.netsys.com  
Message-ID: <20050221173916.H61960@ubzr.zsa.bet>  
Content-Type: TEXT/PLAIN; charset=US-ASCII

Good (morning|afternoon|evening|grief),

I have been trying to reach the Security contact, in fact ANY security contact at Sourceforge for several days now, to no avail.

I \*urgently\* need to speak to someone over there. And, while we're at it, I note publicly that (a) Your switchboard has no option for Security, (b) your operator never answers, (c) the name I was trying for a while is accepted by the automated attendant yet refused when transferred ("That number cannot be reached from here"), and (d) Sending to your role accounts does not get the desired response.

Email to measl@mfn.org or a phone call to the mfn.org role account should both work. I would STRONGLY recommend that someone over there call me whenever they see this, regardless of time of day or night.

--  
Yours,  
J.A. Terranson  
sysadmin@mfn.org  
0xBD4A95BF  
"Quadriplegics think before they write stupid pointless  
shit...because they have to type everything with their noses."  
<http://www.tshirthehell.com/>

-----  
Message: 10  
Date: Mon, 21 Feb 2005 20:19:41 +0800  
From: "Rizwanalikhhan" <rizwanalikhhan74@yahoo.com>  
Subject: [Full-Disclosure] Delivery by mail  
To: "Full-disclosure" <full-disclosure@lists.netsys.com>  
Message-ID: <vyaunvbhudswagtoqer@lists.netsys.com>  
Content-Type: text/plain; charset="us-ascii"  
An HTML attachment was scrubbed...  
URL:  
<http://lists.netsys.com/pipermail/full-disclosure/attachments/20050221/f862d0d3/attachment-0001.htm>

----- next part -----  
A non-text attachment was scrubbed...  
Name: siupd02.cpl  
Type: application/octet-stream  
Size: 32148 bytes  
Desc: not available  
Url :  
<http://lists.netsys.com/pipermail/full-disclosure/attachments/20050221/f862d0d3/siupd02-0001.obj>

## Full-Disclosure: [Full-Disclosure] R: Full-Disclosure Digest, Vol 3, Issue 42

-----  
Message: 11  
Date: Mon, 21 Feb 2005 21:01:29 -0600  
From: H D Moore <fdlist@digitaloffense.net>  
Subject: Re: [Full-Disclosure] Arkeia Network Backup Client Remote  
Access

To: full-disclosure@lists.netsys.com  
Message-ID: <200502212101.29457.felist@digitaloffense.net>  
Content-Type: text/plain; charset="iso-8859-1"  
Just to clarify, the user manual \*does\* mention client security and gives instructions for locking down the Arkeia agent. Unfortunately this is not enabled by default and only restricts access on a per-host basis.  
Appendix B: System Security (not sure how I missed this before)  
<ftp://ftp.arkeia.com/pub/manual/arkeia5/anb/Arkeia User Manual.pdf>

-HD

On Sunday 20 February 2005 14:41, I wrote:  
> Anyone able to connect to TCP port 617 can gain read/write access to  
> the filesystem of any host running the Arkeia agent software.

-----  
Message: 12  
Date: Tue, 22 Feb 2005 00:12:07 -0500  
From: Aaron Horst <anthrax101@gmail.com>  
Subject: [Full-Disclosure] phpBB Fixed full path disclosure in  
username handling - 2.0.11

To: full-disclosure@lists.netsys.com  
Message-ID: <ab13993b05022121122c3c2437@mail.gmail.com>  
Content-Type: text/plain; charset=US-ASCII

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

Hash: SHA1

### I. BACKGROUND

phpBB is a high powered, fully scalable, and highly customizable Open Source bulletin board package. phpBB has a user-friendly interface, simple and straightforward administration panel, and helpful FAQ. Based on the powerful PHP server language and your choice of MySQL, MS-SQL, PostgreSQL or Access/ODBC database servers, phpBB is the ideal free community solution for all web sites.

### II. DESCRIPTION

The `phpbb_clean_username` function has an improper order of execution allowing path and SQL table disclosure. The `substr` function should be called before extra backslash (`\`) characters are stripped from the string to force valid SQL requests. If it is not stripped after the `substr` command, it is possible to remove the second backslash character in a previously addslashes string (`\`). The following code around line 80 in `includes\functions.php` is the problem:

```
$username = htmlspecialchars(trim(trim($username), "\\"));  
$username = substr(str_replace("\\'", "'", $username), 0, 25);  
$username = str_replace("'", "\\'", $username);
```

This is a trivial error, not very worrying. In some configurations this could possibly be used for either cross site scripting or SQL injection, however it does not appear that phpBB v2.0.11 is vulnerable to these attacks.

The following actions are susceptible to this attack:

Login

Password reminder

Add a member to a group

Post by a user who is not logged in

Search by username

Search for username

Send private message

View users profile

To attack any of these actions, attempt to submit the username "ABCDEFGHijklmnopqrstuvwxyz" (Note \ character, there must be

## Full-Disclosure: [Full-Disclosure] R: Full-Disclosure Digest, Vol 3, Issue 42

trailing characters after that character)

### III. FIX

To alleviate this issue, the code around line 80 of includes/functions.php should be changed as follows:

```
$username = substr(htmlspecialchars(str_replace("\\'", "'", trim($username))), 0, 25);  
$username = rtrim($username, "\\");  
$username = str_replace("'", "\\'", $username);
```

An upgrade to phpBB v2.0.12 includes this fix.

### III. ANALYSIS

This report was created based on phpBB v2.0.11. It was discovered on 12/30/04. It was also independently discovered by kaosone+[ONE]+ on 2/19/04, and posted to the bugtraq mailing list.

AnthraX101

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

Version: PGP 8.1 - not licensed for commercial use: www.pgp.com  
iQA/AwUBQhq/Aw4h295M1tC9EQJW2wCgh8jhb97Vc4ZlUkzm/i5VtEiBQlQAoKuH  
UMHOhx0R9jRTU58YO5Oq91C5  
=192I

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

-----  
Message: 13

Date: Tue, 22 Feb 2005 02:18:41 +0800

From: "Rizwanalikhhan" <rizwanalikhhan74@yahoo.com>

Subject: [Full-Disclosure] Registration is accepted

To: "Full-disclosure" <full-disclosure@lists.netsys.com>

Message-ID: <ozpjbjlsflodsusbwea@lists.netsys.com>

Content-Type: text/plain; charset="us-ascii"

An HTML attachment was scrubbed...

URL:

<http://lists.netsys.com/pipermail/full-disclosure/attachments/20050222/29bab00a/attachment.htm>

----- next part -----

A non-text attachment was scrubbed...

Name: zupd02.scr

Type: application/octet-stream

Size: 29227 bytes

Desc: not available

Url :

<http://lists.netsys.com/pipermail/full-disclosure/attachments/20050222/29bab00a/zupd02.obj>

-----  
Full-Disclosure mailing list

Full-Disclosure@lists.netsys.com

<https://lists.netsys.com/mailman/listinfo/full-disclosure>

End of Full-Disclosure Digest, Vol 3, Issue 42

\*\*\*\*\*

-----  
Full-Disclosure - We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>