

مروری بر باگ Cpanel

همان طور که می دانید: متأسفانه هر روز شاهد هک شدن سرورهای بزرگ ایرانی هستیم واقعاً آیا می توان جلوی این حملات را گرفت؟ چرا وقتی می توانیم با کمی وقت گذاشتن و مطالعه جلوی این حملات را بگیریم و از خسارات مادی و معنوی آن جلوگیری کنیم این کار نمی کنیم؟ هر روز چندین هزار **Bug** و **exploit** کشف می شود که ما از آنها بی خبریم. مبحث **Security** چیزی نیست که با یک مدرک ساده ای امنیت شبکه بتوان گفت توانایی کافی در این زمینه را دارا هستیم. هم اکنون به یک سری از توصیه های امنیتی اشاره می کنیم توسط گروه **asquad** ارائه شده است.

برای اینکه مطمئن شوید سرور شما دارای این باگ هست یا نه این فایل **php** را روی سرور خود اجرا کنید.

<http://64.240.171.106/cpanel.php>

این در واقع یک **local exploit** است که برپایه **perl** نوشته شده و یکی از خطرناک ترین **Bug** های آن دسترسی از طریق **nobody shell** به **user** های دیگر است یعنی می توانید تنها با داشتن یک اکانت **ftp** از یک سرور به کل سایت های روی آن سرور دسترسی داشته باشید. حتی می توانید به عنوان یک قربانی از آن استفاده کنید و اهداف خود را از طریق آن سرور پی بگیرید.

متأسفانه **cpanel** به صورت **default** با ماژول **mod_php** کار می کند بنابراین اکثر سرویس دهنده های لینوکس دارای این مشکل هستند. این ماژول امکان دسترسی یک **user** به دیگر **user** های سرور را با استفاده از **UID-Min** (که $uid >= 100$ می باشد) را می دهد.

برای رفع این مشکل باید **apache** را دوباره بر پایه **mod_php suexec** ساخت. (**Build**)
هم اکنون تمام **cpanel** ها از جمله **Releases, current, stables** و حتی **Cpanel 9.3.0-Edge-95** دارای این مشکل هستند. همچنین **OS** های **RedHat 7.3, 8.0, 9, enterprize linux, fedora, freebsd** دارای این مشکل هستند.

بطور کلی وقتی **mo_php** فعال است تمام **script** های **php** با همان کاربر **default web server (nobody)** انجام می شود. این به **user** ها این امکان را می دهد که هر **script** ای که بخواهند برای سرور اجرا کنند و این برای سرورهایی که بیش از ۱ اکانت دارا می باشند و نمی خواهند **user** ها به محدوده هم دیگر دسترسی داشته باشند خطرناک است (به طور کلی **web server** ها) متأسفانه **mod-php** به صورت پیش فرض بر روی **cpanel** نصب می شود (و این مشکل بزرگی است) البته توجه داشته باشید این یک **Bug** یا **exploit** نیست در واقع یک سرویس عادی و طبیعی و مخصوص **mo_php** است که نمی توان آن را منع کرد (مگر با تبدیل آن به **php suexec**)

با این حال باز هم **suexec** ای که همراه **cpanel** ارائه می شود اجازه اجرای کنترل ناشدنی یک **script** ها را به **user** ها می دهد که این با **suexec** ارائه شده در خود **apache** متفاوت است. **Cpanel** برای رفع این مشکل **patch** ای ارائه کرده است.

(home/cpapachebuild/buildapache/suexec.patch)

این **patch** فقط اجازه اجرای این **script** ها را برای **user** های مخصوص **root**، **wheel** را می دهد. فقط مشکلی دارد که اجازه اجرای **shared scripts** را در صورتی که دایرکتوری اصلی آن دارای اجازه **write** برای **user** ها و **group** های دیگر داشته باشد.

علاوه بر این هم چنان یک سری **script** های **perl** و **cgi** وجود دارد که دارای قابلیت **exploit** شدن می باشند. برای مثال:

```
/usr/local/cpanel/bin/proftodvhosts  
/usr/local/cpanel/cgi-sys/addalinh.cgi  
/usr/local/cpanel/cgi-sys/gustbook.cgi  
/usr/local/cpanel/cgi-sys/mchat.cgi  
...
```

برای اطمینان از وجود این **explot** ها بروی سرور خود این دستور را اجرا کنید.

```
Root@server01>find/usr/local / cpanel-user root-group wheel-type f-  
perm+ 1 | xargs-I echo `head-1{| grep - q per | && head -1{| grep-q-r-  
e-T && ls - 1{|1 | sh
```

اگر با اجرای این دستور هیچ پیغامی دریافت نکردید به این معنی که سرور شما کاملاً در برابر این نکات **secure** است. همچنین می توانید از طریق این لینک سرور خود را تست کنید:

<http://64.240.171.106/cpanel.php>

این **Script** سرور شما را در برابر چندین **vulnerability** تست می کند.

این فایل یک سری **php script** با یک **user** معمولی اجرا می کند که باعث اجرا شدن فایل اصلی **tests.pl** می شود. می توانید از این اطلاعات کامل درباره این **tester** دریافت کنید:

<http://www.a-sqvad.co/audit>

اکثر سایت‌ها هر کدام روشی برای **patch** کردن این **Bug** ها ارائه کردن ولی اکثراً کامل نیستند و یا دارای ایراد هستند. در زیر به چند روش اشاره می‌کنیم:

۱-بهترین کار (که باعث از بین رفتن مشکلات دیگر نیز می‌شود) تغییر ماژول **php** از **mod-php** به **mod-phpsuexec** می‌باشد: راه اول: **apache** را **compile** کنید
(«شماره ۲» **/scripts/easyapache**)

ولی مواظب باشید بسیاری از **permission** ها و **owner ships** ها برپایه **phpscripts** است و این کار شما ممکن است باعث ایجاد اختلال در بعضی سایت‌ها شود.
*با مسئولیت خود این کار را انجام دهید.

2-فایل **patch** را پاک کنید بعد از اجرای **buildapache**

(**/home/cdapachbuidl/buildapach/suexea.patch**)

ولی توجه داشته باشید قبل از انتخاب راه اول: این راه سرور شما را **secure** می‌کند اما ممکن است مشکلاتی ایجاد کند که بستگی به **shared script** های شما و **user** ها و سایت‌های روی سرور شما دارد. با این حال می‌توانید با خود **mod-php** هم فعلاً مشکل را حل کنید.

شاید بهتر باشد **suexec.patch** اصلاح کنید تا پوشه‌های اصلی را برای این مشکلات امنیتی **Scan** کند (قبل از اینکه اجازه اجرای **Script** را بدهد)

3-اگر نمی‌توانید راه اول را انتخاب کنید یا نگران ایجاد مشکل بر روی سرور و یا عوض کردن **php engine** خود هستید می‌توانید خود با تغییر **Script** های **perl** برای **root.wheel** این

مشکل را از بین ببرید در زیر روشی برای این کار ذکر کرده ایم.

کافی است فقط یک **(-T)** به آن‌ها اضافه کنیم.

```
-----snip -----
---/usr/local/cpanel/bin/proftpdvhosts.o    2003-02-22
09:38:52.000000000 - 0700
+++/usr/local/cpanel/bin/proftpdvhosts    2004-05-27
00:10:20.000000000 - 0600
@@-1 , 5 +1 , 6 @@
-#!/usr/bin/perl
+#!/usr/bin/perl-T

+% ENV = (PATH => "/usr/bin:/bin:/sbin:/usr/sbin");
BEGIN {
    Push @ INC, "/scripts");
}
---- snap ----
```

فقط مشکلی که در این روش وجود دارد این است که با انجام این **taint clean Script** ها بعد از هر **cpanel, update (/Scripts/upcp)** تمام این تنظیمات از بین می رود و دوباره باید انجام گردد.

۴- راه راحت تر این است که **owner ship** تمام **untaint script** ها را به **root wheel** تبدیل کنید.

Chgrp root / usr/ local/cpanel/ hin / proft pdv hosts

بنابراین شما احتیاجی به **fix** کردن هیچ **Script** ای ندارید. فقط کافی است **Schared Script** ها را به **root wheel** تبدیل کنید. بنابراین برای اجرا شدن آنها حتماً باید با **group** **root wheel** وارد شوند.

پیشنهاد می کنم برای اینکه خیال خود را راحت کنید تمام **perl script** های قابل اجرا را که مال **root.wheel** هستند را **taint clean** کنید اگر نمی توانید این کار را کنید آن را پاک کنید یا **ownership** آن را به **root.wheel** تغییر دهید یا **Chmod** آنها را روی صفر قرار دهید.

در کل Cpanel همیشه خود دارای مشکلات بسیار بوده است و خواهد بود این مشکل شامل تمام

نرم افزارهای 3dparty و opensource می باشد. بهترین کار این است که admin یک سرور

روز به سایت Security news سر بزنند و از اخبار جدید اطلاع یابد.

Performing white box security audit...

1. **PASSED:** cPanel INSTALLED (9.3.0-RELEASE_5)
2. **FAILED:** Privileged UID Vulnerability Check (99) [Explain](#)
3. **FAILED:** nobody execution [Explain](#)
4. **FAILED:** Stealth Snoop Vulnerability [/home/barg] [Explain](#)
5. **PASSED:** Simple \$HOME Scanning [/home/barg]
6. **PASSED:** Group \$HOME Scanning [/home/barg]
7. **PASSED:** Root /home scanning
8. **PASSED:** Simple WEBROOT Protection
9. **FAILED:** Real WEBROOT Protection [Explain](#)
10. **FAILED:** suEXEC mod_php Taint Vulnerability Test [Explain](#)

```
EXEC [id -a] as [barg]:
```

```
uid=32016(barg) gid=32016(barg) groups=32016(barg)
```

11. **FAILED:** One or more insecure cPanel configurations were detected. Visit [A-Squad.Com](#) for details on where to find more secure cPanel hosting.

Username:

Password: (not required)

Command:

Test Execution

منابع:

1-http: //www.security focus.com/archive/1/365328

2-http: //cve.mitre.org/cgi-bin/cvename.cgi?name-CAN-2004-0529

3-cPanel's Internal Ticket Request: # 17703 (no public URL)

4-http: //www.a-squad.com/audit/

5-http://bugzilla.cpanel.net/show_bug.cgi?id=668

توجه داشته باشید ۲ مشکل را بررسی کردیم یکی مربوط به **mod-phpsuexec** می باشد. دیگری مربوط به **/usr/local/apach/bin/suexec** همراه با **mod-php** است. برای اطلاعات بیشتر به این **link** توجه کنید:

<http://cve.mitre.org/cgi-bin/cvename.cgi?CVE-2004-0490>

اگر سوال یا اشکال و ایرادی وجود داشت با کمال میل در خدمت دوستان و علاقه‌مندان عزیز می باشیم.

Support@cypherHost.com

فرشاد اسماعیلیان

CypherHost مدیر امنیتی