**Đề tài nghiên cứu: Khai thác lỗ hổng trên WinRar và Apache**

* 1. Mục tiêu
* Nghiên cứu và phân tích lỗ hổng bảo mật CVE-2023-38831 (WinRar)
* Nghiên cứu và phân tích lỗ hổng bảo mật CVE-2018-20250 (WinRar)
* Nghiên cứu và phân tích lỗ hổng bảo mật CVE-2021-43617 (Apache)
* Xác định cơ chế tấn công, điều kiện cần, và tác động của lỗ hổng.
* Đề xuất biện pháp bảo vệ và giảm thiểu nguy cơ cho hệ thống sử dụng WinRAR

Bài toán giải quyết

Lỗ hổng thực thi mã CVE-2023-38831 và CVE-2018-20250 là lỗ hổng nghiêm trọng trong WinRAR. Lỗ hổng này cho phép kẻ tấn công thực thi mã tùy ý khi nạn nhân giải nén tập tin bị ảnh hưởng.

* 1. Tổng quan vấn đề nghiên cứu
     + 1. WinRAR:

Là một phần mềm nén và giải nén tập tin được sử dụng rộng rãi trên máy tính. WinRAR cho phép người dùng nén các tập tin và thư mục để giảm kích thước của chúng và truyền chúng dễ dàng hơn hoặc bảo vệ chúng bằng mật mã. WinRAR còn cung cấp nhiều tùy chọn và công cụ hữu ích cho việc quản lý tập tin nén.

Tính năng của Winrar:

* Nén tập tin: WinRAR có thể nén các tập tin thành các tập tin RAR hoặc ZIP với tỉ lệ nén tốt và nhanh chóng.
* Giải nén tập tin: đáp ứng việc giải nén các tập tin RAR, ZIP, và các định dạng tập tin nén khác như 7Z, ISO,... Tính năng tự động giải nén, sau khi tải về, giúp tiết kiệm thời gian và công sức cho người dùng.
* Tạo nhiều tập tin nhỏ từ một tập tin lớn, giúp cho việc truyền tải và lưu trữ dữ liệu trở nên dễ dàng hơn.
* WinRAR cung cấp tính năng mã hóa dữ liệu bảo mật cho các tập tin nén, giúp bảo vệ thông tin cá nhân và công việc của người dùng.
* Tạo mật khẩu cho tập tin nén giúp bảo vệ dữ liệu trong tập tin nén khỏi sự truy cập trái phép.
* Tạo nội dung tự động cho các tập tin nén, giúp người dùng tìm kiếm và sử dụng tập tin dễ dàng hơn.
* WinRAR hỗ trợ tập tin lớn, giúp người dùng nén và giải nén các tập tin có dung lượng lớn một cách dễ dàng và nhanh chóng, Tối ưu hóa tốc độ nén bằng cách sử dụng các thuật toán nén hiệu quả và tối ưu hóa sử dụng tài nguyên máy tính.
* WinRAR hỗ trợ đa ngôn ngữ, giúp người dùng sử dụng phần mềm một cách dễ dàng và tiện lợi, không cần phải sử dụng một ngôn ngữ cụ thể.
  + - 1. Apache HTTP Server (thường được gọi là Apache)

Là một máy chủ web mã nguồn mở phổ biến, được sử dụng rộng rãi trên Internet để phục vụ các trang web và ứng dụng web.

Apache HTTP Server có thể xử lý các yêu cầu HTTP từ các trình duyệt web và gửi lại các trang web, tệp tin và dữ liệu tương ứng. Nó hỗ trợ các giao thức web phổ biến như HTTP, HTTPS, và các giao thức khác như FTP và SMTP. Apache cung cấp các tính năng như xử lý đa luồng, bảo mật, cấu hình linh hoạt và khả năng mở rộng.

Apache HTTP Server cung cấp tính năng nổi bật quan trọng sau:

1. Bảo mật: mạnh mẽ như hỗ trợ SSL/TLS để mã hóa giao tiếp, hạn chế truy cập dựa trên địa chỉ IP hoặc tên miền, kiểm soát truy cập dựa trên quyền và chứng chỉ xác thực. Chống lại các cuộc tấn công từ chối dịch vụ (DoS) và tấn công Cross-Site Scripting (XSS).
2. Mở rộng: cho phép người dùng tùy chỉnh và cấu hình linh hoạt với các tệp cấu hình và phần mở rộng như cổng lắng nghe, máy chủ ảo, cấu hình SSL/TLS và module, plugin để thêm tính năng, khả năng cho máy cho web.
3. Hiệu suất cao: Apache được tối ưu hóa để cung cấp hiệu suất cao và xử lý đồng thời nhiều yêu cầu từ nhiều nguồn khác nhau.
4. Quản lý tài nguyên: Apache cho phép quản lý tài nguyên như băng thông, số lượng kết nối và tài nguyên máy chủ để đảm bảo hiệu suất và ổn định.
5. Cộng đồng hỗ trợ: Apache được phát triển và duy trì bởi Apache Software Foundation, có một cộng đồng lớn và nhiều nguồn tài liệu hỗ trợ để giúp người dùng trong việc triển khai và quản lý máy chủ web.
   1. Mô tả lỗ hổng
      * 1. CVE-2023-38831

RARLAB WinRAR trước 6.23 cho phép kẻ tấn công thực thi mã tùy ý khi người dùng cố gắng xem một tệp vô hại trong kho lưu trữ ZIP. Sự cố xảy ra do kho lưu trữ ZIP có thể bao gồm một tệp lành tính (chẳng hạn như tệp .JPG thông thường) và một thư mục có cùng tên với tệp lành tính và nội dung của thư mục (có thể bao gồm nội dung thực thi) được xử lý trong khi cố gắng chỉ truy cập vào tệp lành tính. CVE này đã được khai thác trong tự nhiên từ tháng 4 đến tháng 10 năm 2023.

* + - 1. CVE-2018-20250

Trong các phiên bản WinRAR trước và bao gồm phiên bản 5.61, có lỗ hổng **path traversal** khi tạo trường tên tệp ở định dạng ACE (trong UNACEV2.dll). Khi trường tên tệp được xử lý bằng các mẫu cụ thể, thư mục đích sẽ bị bỏ qua, do đó coi tên tệp là đường dẫn tuyệt đối. Mô-đun này sẽ cố gắng trích xuất một payload vào thư mục khởi động của người dùng hiện tại. Nó bị giới hạn đến mức chúng ta chỉ có thể quay lại một thư mục. Do đó, để cách khai thác này hoạt động bình thường, người dùng phải giải nén tệp RAR được cung cấp từ một thư mục trong thư mục hồ sơ người dùng (ví dụ: Desktop hoặc Dowload). Cần phải khởi động lại người dùng để có được shell.

* + - 1. CVE-2021-43617

Lỗ hổng liên quan đến việc bypass upload file của framework laravel (< 8.72.0). Đặc biệt, lỗ hổng này chỉ ảnh hưởng đến các ứng dụng lavarel chạy trên hệ điều hành Debian. Các ứng dụng trên hệ điều hành khác không bị ảnh hưởng. Team Lavarel đã đưa ra bản vá vào phiên bản (8.73.2), tuy nhiên theo tác giả của CVE này, lỗ hổng nằm ở việc bypass cơ chế kiểm tra tập tin được tải lên bởi người dùng.

Cụ thể hơn thì Laravel Framework từ 8.70.2 trở xuống không chặn đủ việc tải lên nội dung PHP thực thi vì Illuminate / Validation / Concerns / ValidatesAttributes.php không kiểm tra các tệp ".phar", được xử lý dưới dạng ứng dụng / x-httpd-php trên hệ thống dựa trên Debian.

* 1. Khảo sát vấn đề + mô hình đề xuất
     + 1. Phân tích lỗ hổng CVE-2023-38831

Để khai thác lỗ hổng này, kẻ tấn công cần tạo một tệp ZIP có chứa một thư mục có cùng tên với một tệp vô hại. Thư mục này sau đó chứa một tệp thực thi độc hại. Khi nạn nhân cố gắng xem tệp vô hại, WinRAR sẽ cố gắng mở thư mục và thực thi tệp thực thi độc hại.

Để khai thác lỗ hổng CVE-2023-38831, kẻ tấn công cần thực hiện các bước sau:

* Xây dựng một keylogger cơ bản bằng python3
* Chuyển sang ngôn ngữ Computer
* Chèn chương trình này vào phần mềm Winrar
* Tiến hành lây nhiễm trên máy nạn nhân

**Mô hình triển khai**

Mô hình:

* Một máy windows để xây dựng phần mềm độc hại trên WinRAR
* Một máy windows nạn nhân khi nhận file từ kẻ tấn công

Để khai thác lỗ hổng, ta có thể sử dụng các cách sau:

* Viết mã khai thác bằng python
  + - 1. Phân tích lỗ hổng CVE-2018-20250

Để khai thác lỗ hổng này, kẻ tấn công cần tạo một file RAR có file mã độc đính kèm. Khi victim cố gắng xem tệp vô hại, WinRAR sẽ cố gắng mở thư mục và thực thi tệp thực thi độc hại.

Để khai thác lỗ hổng CVE-2018-20250, kẻ tấn công cần thực hiện các bước sau:

* Tạo file RAR chứa file độc hại đính kèm
* Gửi file đến cho victim
* Victim extract file RAR và restart lại máy
* Tiến hành khai thác trên máy nạn nhân

**Mô hình triển khai**

Mô hình:

* Một máy windows để xây dựng phần mềm độc hại trên WinRAR
* Một máy windows nạn nhân khi nhận file từ kẻ tấn công
* Một máy kali linux thực hiện tấn công
  + - 1. Phân tích lỗ hổng CVE-2021-43617

**Nguyên nhân dẫn đến lỗ hổng**

Mặc định, lavarel sẽ cấm người dùng tải lên các tập tin php. Hàm kiểm tra nằm tại Illuminate/Validation/Concerns/ValidatesAttributes.php

protected function shouldBlockPhpUpload($value, $parameters){

if (in\_array('php', $parameters)){

return *false*;

}

$phpExtensions = ['php', 'php3', 'php4', 'php5', 'phtml', ];

return ($value instanceof UploadedFile)

? in\_array(trim(strtolower($value->getClientOriginalExtension())), $phpExtensions)

: in\_array(trim(strtolower($value->getExtension())), $phpExtensions);

}

Laravel đã bỏ qua các tập tin có đuôi .phar.

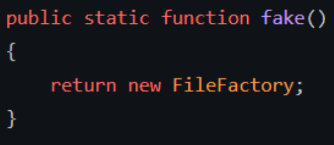
Và đoạn code trả về

return ($value instanceof UploadedFile)

? in\_array(trim(strtolower($value->getClientOriginalExtension())), $phpExtensions)

: in\_array(trim(strtolower($value->getExtension())), $phpExtensions);

File tải lên sẽ được luân chyển qua UploadFile. Tại Uploadfile sẽ đi qua function fake()



Bản thân function này sẽ trả về cho ta 1 File Factory. Nó làm nhiệm vụ đọc dữ liệu upload lên và tạo 1 tệp fake tương tự để hiển thị kết quả cho người dùng.

Ngoài ra, việc Debian lại mặc định hỗ trợ thực thi các tập tin .phar. bạn có thể kiểm tra Tập tin cấu hình php trên apache /etc/apache2/mods-# application/x-httpd-php phtml pht php

# application/x-httpd-php3 php3

# application/x-httpd-php4 php4

# application/x-httpd-php5 php

<FilesMatch ".+\.ph(p[3457]?|t|tml)$">

SetHandler application/x-httpd-php

</FilesMatch>

# application/x-httpd-php-source phps

Require all denied

</FilesMatch>

# Deny access to files without filename (e.g. '.php')

<FilesMatch "^\.ph(p[3457]?|t|tml|ps)$">

Require all denied

</FilesMatch>

Từ 2 nguyên nhân trên kẻ tấn công có thể tạo payload và lưu chúng dưới dạng phar extentsion để tấn công người dùng sử dụng debian.

Ảnh hưởng của lỗ hổng

Tất nhiên, khi upload được file phar và còn executed được code thì ảnh hưởng xấu nhất của lỗ hổng sẽ là thực thi mã từ xa và chiếm quyền máy chủ.

Để khai thác lỗ hổng CVE-2021-43617, kẻ tấn công cần thực hiện:

Upload 1 hình ảnh bình thường trước

Tạo 1 file đuôi .phar

Lắng nghe trên cổng đã tạo trong payload

Rồi upload file .phar lên

**Mô hình triển khai**

Mô hình:

- 1 máy chạy Debian

- 1 máy tấn công

Để khai thác, ta sử dụng

- Môi trường để triển khai

* 1. Thực nghiệm triển khai giải pháp
     + 1. CVE-2023-38831

Mô tả về từng máy trong mô hình thực nghiệm

* Máy nạn nhân: Máy windows sử dụng WinRAR phiên bản trước 6.23
* Máy tấn công: Máy windows của kẻ tấn công

Đưa ra các kịch bản: mục tiêu, tiến hành, đánh giá

Kịch bản: Kẻ tấn công thực thi mã độc thông qua kho lưu trữ ZIP được tạo riêng. Lỗ hổng phát sinh do việc xử lý sai các kho lưu trữ ZIP chứa các tệp lành tính, chẳng hạn như tài liệu .PDF thông thường, cùng với các thư mục có cùng tên. Khi người dùng cố gắng truy cập vào tệp lành tính, kho lưu trữ có thể bao gồm một thư mục có tên tương tự chứa nội dung thực thi. Nội dung độc hại trong thư mục này được xử lý trong quá trình cố gắng truy cập vào tệp lành tính.

* + - 1. CVE-2018-20250

Mô tả về từng máy trong mô hình thực nghiệm

* Máy chủ victim: Máy win7 đang sử dụng Winrar5.5
* Máy tạo file rar : Máy HDH Win
* Máy tấn công: máy kali của attacker

Đưa ra các kịch bản: mục tiêu, tiến hành, đánh giá

Kịch bản tấn công: Một user A đang sử dụng Winrar có phiên bản dính lỗ hổng, một attcker đang nhắm mục tiêu user A và gửi file RAR có mã độc cho victim.

* + - 1. CVE-2021-43617

Mô tả về từng máy trong mô hình thực nghiệm

* Máy chủ Apache: Máy chủ Debian chạy Laravel từ 8.70.2 trở xuống
* Máy tấn công: máy kali của attcker

Đưa ra các kịch bản: mục tiêu, tiến hành, đánh giá

Kịch bản tấn công: Một công ty A đang sử dụng Laravel có phiên bản đang dính cve, một attcker đang nhắm mục tiêu của công ty A với mục tiêu tải lên nội dung PHP gây hại.

**Kết luận**

Qua nghiên cứu, chúng em đã xác định được lỗ hổng thực thi mã (CVE-2023-38831 và CVE-2018-20250) trong WinRAR và lỗ hổng khai thác việc bypass upload file của framework LARAVEL (CVE-2021-43617) . Lỗ hổng này có thể được khai thác để cho phép kẻ tấn công thực thi mã tùy ý trên máy chủ bị ảnh hưởng.

Để ngăn chặn lỗ hổng này, người dùng cần cập nhật WinRAR phiên bản để tránh lỗ hổng , phiên bản framework LARAVEL từ 8.70.2 trở lên .

Ngoài ra, người dùng cũng cần nâng cao nhận thức về bảo mật, tránh tải về những file nén không rõ nguồn gốc , tránh truy cập vào các trang web không đáng tin cậy và sử dụng các phần mềm bảo mật để bảo vệ máy tính.

**Hạn chế**:

**Hướng phát triển (dự định) cho nghiên cứu trong tương lai:**

* Nghiên cứu sâu hơn về lỗ hổng, tìm ra các cách khai thác mới và hiệu quả hơn.
* Tìm ra các cách để phát hiện và ngăn chặn lỗ hổng này một cách tự động.

**Tài liệu tham khảo**

CVE-2023-38831

* <https://nvd.nist.gov/vuln/detail/CVE-2023-38831>
* <https://packetstormsecurity.com/files/174573/WinRAR-Remote-Code-Execution.html>
* <https://www.bleepingcomputer.com/news/security/winrar-zero-day-exploited-since-april-to-hack-trading-accounts/>
* <https://www.group-ib.com/blog/cve-2023-38831-winrar-zero-day/>
* <https://github.com/HDCE-inc/CVE-2023-38831>
* <https://blog.google/threat-analysis-group/government-backed-actors-exploiting-winrar-vulnerability/>
* <https://whitehat.vn/threads/tao-malware-don-gian-voi-cve-2023-38831.17474/>

CVE-2018-20250

* <https://nvd.nist.gov/vuln/detail/CVE-2018-20250>
* <https://www.cvedetails.com/cve/CVE-2018-20250/>
* <https://research.checkpoint.com/2019/extracting-code-execution-from-winrar/>
* [Demo khai thác lỗ hổng WinRAR CVE-2018-20250 | WhiteHat.vn](https://whitehat.vn/threads/demo-khai-thac-lo-hong-winrar-cve-2018-20250.12371/)
* <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20250>

CVE-2021-43617

* <https://whitehat.vn/threads/phan-tich-va-huong-dan-trien-khai-cve-2021-43617-phan-1.16286/>
* <https://whitehat.vn/threads/phan-tich-va-huong-dan-trien-khai-cve-2021-43617-phan-2.16627/>
* <https://vuldb.com/?id.186652>
* <https://nvd.nist.gov/vuln/detail/CVE-2021-43617>