Pwn2Own 解碼

廠商視角的弱點反思

Synology Product Developer

吳勃興

Synology

whoami

- 吳勃興
- Synology Product Developer
- Security Incident Response Team

為什麼會有這個議程

Pwn2Own

- 全球頂尖攻防競賽
  - Pre-auth RCE
- Synology 自 2020 年起便持續參與
  - Tokyo 2020
  - Austin 2021
  - Toronto 2022
  - Toronto 2023
  - Ireland 2024

Pwn2Own Ireland 2024

不同於往年

- 新產品線加入競賽
- 讓 scope 變得更大

For the Synology DiskStation target, the following packages will be installed and are in scope for contest:

- MailPlus
- Drive
- Virtual Machine Manager
- Snapshot Replication
- Surveillance Station
- Photos

Pwn2Own 2024 Result

收穫良多的一年

		SUCCESS	COLLISION	FAILURE	WITHDRAWN
Network Attached Storage (NAS)	**DiskStation**	3	0	1	0
	BeeStation	3	1	1	0
Surveillance Systems		1	0	2	1
Small Office / Home Office (SOHO) Smash-up		0	0	1	0

Pwn2Own 2024 Result

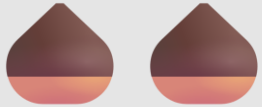
收穫良多的一年

研究者如何發現？ 我們如何改進？

		SUCCESS	COLLISION	FAILURE	WITHDRAWN
Network Attached Storage (NAS)	**DiskStation**	3	0	1	0
	BeeStation	3	1	1	0
Surveillance Systems		1	0	2	1
Small Office / Home Office (SOHO) Smash-up		0	0	1	0

案例探討

Synology

來點例子 

- Off-by-one Error
- Improper Encoding of Output

Off-by-one Error

Replication Service

Synology

Replication Service

- 將拍攝的快照從來源複寫至目的地
- 無法單獨運作，必須依附其他提供快照功能的套件

For the Synology DiskStation target, the following packages will be installed and are in scope for contest:

- MailPlus
- Drive
- Virtual Machine Manager
- Snapshot Replication
- Surveillance Station
- Photos

Synology

Off-by-one Error

1. 尋找入口
2. 了解過程
3. 發現漏洞
4. Exploit

Off-by-one Error

1. 尋找入口
2. 了解過程
3. 發現漏洞
4. Exploit

開了哪些 port

```
tcp6       0      0 :::3261                 :::*                    LISTEN      -
tcp6       0      0 :::445                  :::*                    LISTEN      12153/smbd
tcp6       0      0 :::5566                 :::*                    LISTEN      14331/synobtrfsrepl
tcp6       0      0 :::3263                 :::*                    LISTEN      -
tcp6       0      0 :::3264                 :::*                    LISTEN      -
tcp6       0      0 :::3265                 :::*                    LISTEN      13156/scsi_plugin_s
tcp6       0      0 :::2049                 :::*                    LISTEN      -
tcp6       0      0 :::5000                 :::*                    LISTEN      9553/nginx: master
tcp6       0      0 :::5001                 :::*                    LISTEN      9553/nginx: master
tcp6       0      0 :::139                  :::*                    LISTEN      12152/smbd
```

Off-by-one Error

1. 尋找入口
2. 了解過程
3. 發現漏洞
4. Exploit

逆起來

```
struct ReplicaCmdHeader {
    uint32_t cmd;
    uint32_t seq;
    uint32_t len;
};

struct ReplicaCmd {
    struct ReplicaCmdHeader header;
    char *data;
};
```

Off-by-one Error

1. 尋找入口
2. 了解過程
3. 發現漏洞
4. Exploit

```
int recvCmd(struct ReplicaCmd &xxx) {
    int retval = SNAPREPLICA_ERR_GENERIC;

    if (SNAPREPLICA_ERR_NONE != (retval = receiveMessage(xxx))) {
        goto Exit;
    }
    if (xxx.header.len > RECV_BUF_SIZE) {
        goto Exit;
    }
    // Read data
}

int runCmdLoop(bool &xxx) {
    int retval = SNAPREPLICA_ERR_GENERIC;

    while (xxx) {
        if (SNAPREPLICA_ERR_NONE != (retval = recvCmd(xxx))) {
            goto Exit;
        }
        if (CMD_SEND != xxx.header.cmd) {
            xxx.data[xxx.header.len] = '\0';
        }
    }
}
```

Off-by-one Error

1. 尋找入口
2. 了解過程
3. 發現漏洞
4. Exploit

```
struct ReplicaBufPool {
    uint8_t bufIdx = 0;
    char buf[REPLICA_BUF_POOL_SIZE][RECV_BUF_SIZE] = {0};
    uint32_t bufLen[REPLICA_BUF_POOL_SIZE] = {0};
};
```

```
int recvCmd(struct ReplicaCmd &xxx) {
    int retval = SNAPREPLICA_ERR_GENERIC;

    if (SNAPREPLICA_ERR_NONE != (retval = receiveMessage(xxx))) {
        goto Exit;
    }
    if (xxx.header.len > RECV_BUF_SIZE) {
        goto Exit;
    }
    // Read data
}

int runCmdLoop(bool &xxx) {
    int retval = SNAPREPLICA_ERR_GENERIC;

    while (xxx) {
        if (SNAPREPLICA_ERR_NONE != (retval = recvCmd(xxx))) {
            goto Exit;
        }
        if (CMD_SEND != xxx.header.cmd) {
            xxx.data[xxx.header.len] = '\0';
        }
    }
}
```


Synology

Off-by-one Error

1. 尋找入口
2. 了解過程
3. 發現漏洞
4. Exploit

```
int recvCmd(struct ReplicaCmd &xxx) {
    int retval = SNAPREPLICA_ERR_GENERIC;

    if (SNAPREPLICA_ERR_NONE != (retval = receiveMessage(xxx))) {
        goto Exit;
    }
    if (xxx.header.len > RECV_BUF_SIZE) {
        goto Exit;
    }
    // Read data
}

int runCmdLoop(bool &xxx) {
    int retval = SNAPREPLICA_ERR_GENERIC;

    while (xxx) {
        if (SNAPREPLICA_ERR_NONE != (retval = recvCmd(xxx))) {
            goto Exit;
        }
        if (CMD_SEND != xxx.header.cmd) {
            xxx.data[xxx.header.len] = '\0';
        }
    }
}
```

Off-by-one Error

1. 尋找入口
2. 了解過程
3. 發現漏洞
4. Exploit

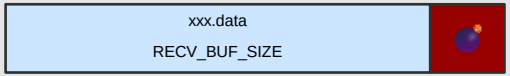
```
struct ReplicaBufPool {
    uint8_t bufIdx = 0;
    char buf[REPLICA_BUF_POOL_SIZE][RECV_BUF_SIZE] = {0};
    uint32_t bufLen[REPLICA_BUF_POOL_SIZE] = {0};
};
```

```
int recvCmd(struct ReplicaCmd &xxx) {
    int retval = SNAPREPLICA_ERR_GENERIC;

    if (SNAPREPLICA_ERR_NONE != (retval = receiveMessage(xxx))) {
        goto Exit;
    }
    if (xxx.header.len > RECV_BUF_SIZE) {
        goto Exit;
    }
    // Read data
}

int runCmdLoop(bool &xxx) {
    int retval = SNAPREPLICA_ERR_GENERIC;

    while (xxx) {
        if (SNAPREPLICA_ERR_NONE != (retval = recvCmd(xxx))) {
            goto Exit;
        }
        if (CMD_SEND != xxx.header.cmd) {
            xxx.data[xxx.header.len] = '\0';
        }
    }
}
```


Synology

Off-by-one Error

1. 尋找入口
2. 了解過程
3. 發現漏洞
4. Exploit




```
int recvCmd(struct ReplicaCmd &xxx) {
    int retval = SNAPREPLICA_ERR_GENERIC;

    if (SNAPREPLICA_ERR_NONE != (retval = receiveMessage(xxx))) {
        goto Exit;
    }
    if (xxx.header.len > RECV_BUF_SIZE) {
        goto Exit;
    }
    // Read data
}

int runCmdLoop(bool &xxx) {
    int retval = SNAPREPLICA_ERR_GENERIC;

    while (xxx) {
        if (SNAPREPLICA_ERR_NONE != (retval = recvCmd(xxx))) {
            goto Exit;
        }
        if (CMD_SEND != xxx.header.cmd) {
            xxx.data[xxx.header.len] = '\0';
        }
    }
}
```


Synology

Off-by-one Error

1. 尋找入口
2. 了解過程
3. 發現漏洞
4. Exploit


```
int recvCmd(struct ReplicaCmd &xxx) {
    int retval = SNAPREPLICA_ERR_GENERIC;

    if (SNAPREPLICA_ERR_NONE != (retval = receiveMessage(xxx))) {
        goto Exit;
    }
    if (xxx.header.len > RECV_BUF_SIZE) {
        goto Exit;
    }
    // Read data
}

int runCmdLoop(bool &xxx) {
    int retval = SNAPREPLICA_ERR_GENERIC;

    while (xxx) {
        if (SNAPREPLICA_ERR_NONE != (retval = recvCmd(xxx))) {
            goto Exit;
        }
        if (CMD_SEND != xxx.header.cmd) {
            xxx.data[xxx.header.len] = '\0';
        }
    }
}
```


Synology

Off-by-one Error

1. 尋找入口
2. 了解過程
3. 發現漏洞
4. Exploit

- Create information leak
  - Defeat ASLR
  - Leak BSS address
- Hijack control flow
  - Overwrite GOT entry

Off-by-one Error

1. 尋找入口
2. 了解過程
3. 發現漏洞
4. Exploit

- Create information leak
  - Defeat ASLR
  - Leak BSS address
- Hijack control flow
  - Overwrite GOT entry

Off-by-one Error

1. 尋找入口
2. 了解過程
3. 發現漏洞
4. Exploit

- Create information leak
  - Defeat ASLR
  - Leak BSS address
- Hijack control flow
  - Overwrite GOT entry

Off-by-one Error

1. 尋找入口
2. 了解過程
3. 發現漏洞
4. Exploit

- Create information leak
  - Defeat ASLR
  - Leak BSS address
- Hijack control flow
  - Overwrite GOT entry

Off-by-one Error

關鍵疏漏

- 函數返回值不夠準確
- 記憶體管理不夠嚴謹

Off-by-one Error

關鍵疏漏

- 函數返回值不夠準確
- 記憶體管理不夠嚴謹

```
int recvCmd(struct ReplicaCmd &xxx) {
    int retval = SNAPREPLICA_ERR_GENERIC;

    if (SNAPREPLICA_ERR_NONE != (retval = receiveMessage(xxx))) {
        goto Exit;
    }
    if (xxx.header.len > RECV_BUF_SIZE) {
        goto Exit;
    }
    // Read data
}

int runCmdLoop(bool &xxx) {
    int retval = SNAPREPLICA_ERR_GENERIC;

    while (xxx) {
        if (SNAPREPLICA_ERR_NONE != (retval = recvCmd(xxx))) {
            goto Exit;
        }
        if (CMD_SEND != xxx.header.cmd) {
            xxx.data[xxx.header.len] = '\0';
        }
    }
}
```

Off-by-one Error

關鍵疏漏

- 函數返回值不夠準確
- 記憶體管理不夠嚴謹

```
struct ReplicaBufPool {
    uint8_t bufIdx = 0;
    char buf[REPLICA_BUF_POOL_SIZE][RECV_BUF_SIZE] = {0};
    uint32_t bufLen[REPLICA_BUF_POOL_SIZE] = {0};
};
```

```
int recvCmd(struct ReplicaCmd &xxx) {
    int retval = SNAPREPLICA_ERR_GENERIC;

    if (SNAPREPLICA_ERR_NONE != (retval = receiveMessage(xxx))) {
        goto Exit;
    }
    if (xxx.header.len > RECV_BUF_SIZE) {
        goto Exit;
    }
    // Read data
}

int runCmdLoop(bool &xxx) {
    int retval = SNAPREPLICA_ERR_GENERIC;

    while (xxx) {
        if (SNAPREPLICA_ERR_NONE != (retval = recvCmd(xxx))) {
            goto Exit;
        }
        if (CMD_SEND != xxx.header.cmd) {
            xxx.data[xxx.header.len] = '\0';
        }
    }
}
```

Off-by-one Error

關鍵疏漏

- 函數返回值不夠準確
- 記憶體管理不夠嚴謹

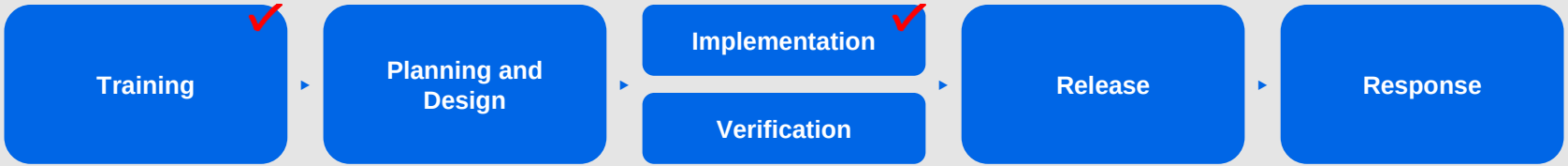
修復方式

- 重新審閱相關實作
  - 緩衝區大小
  - 函數返回值

Off-by-one Error

改進方式

- Internal Training
- SAST
- Full RELRO



Synology

Off-by-one Error

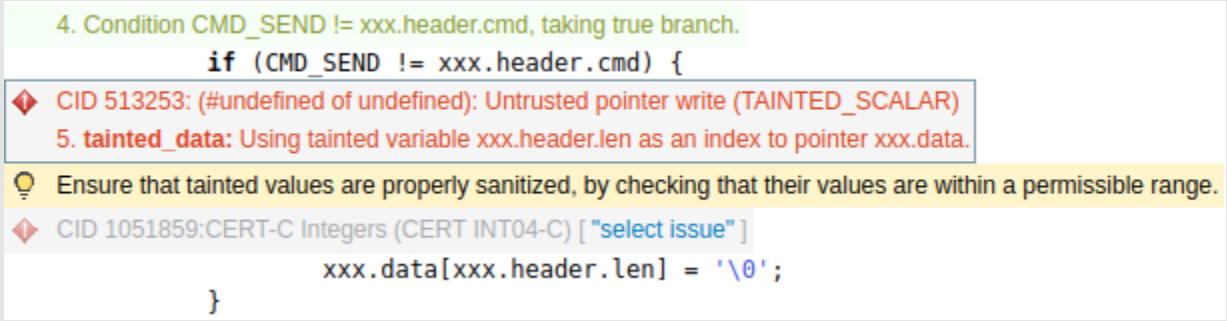
改進方式

- Internal Training
  - Newbie training (e.g. CTF style lab)
  - Regular sharing talk
- SAST
- Full RELRO

Off-by-one Error

改進方式

- Internal Training
- SAST
  - Medium issue
- Full RELRO



Synology

Off-by-one Error

改進方式

- Internal Training
- SAST
- Full RELRO
  - Bye, GOT hijacking

```
$ checksec file -l ./libc.so.6 synobtrfsreplicad -o json | jq .
[
  {
    "checks": {
      "canary": "Canary Found",
      "fortified": "1",
      "fortify_source": "Yes",
      "fortifyable": "1",
      "nx": "NX enabled",
      "pie": "PIE Enabled",
      "relro": "Partial RELRO",
      "rpath": "RPATH",
      "runpath": "No RUNPATH",
      "symbols": "61 symbols"
    },
    "name": "synobtrfsreplicad"
  }
]
```

Off-by-one Error

評估中的改進方式

- libc++ hardening mode
- Rust

Improper Encoding of Output

Plugin Framework

Synology®

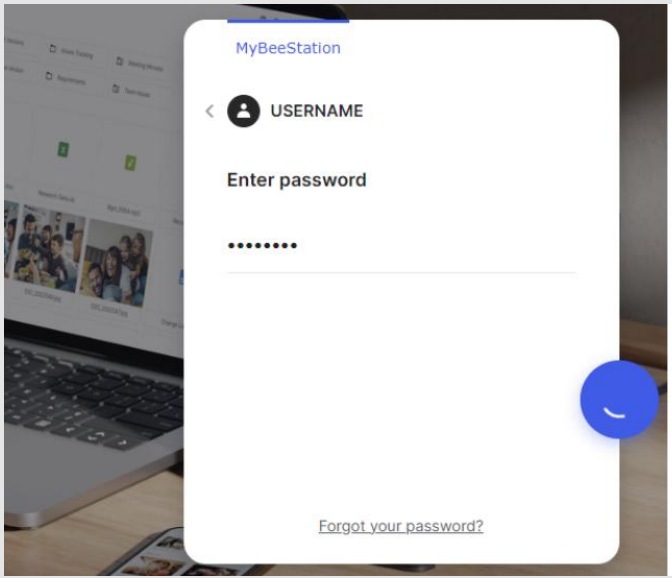
Improper Encoding of Output

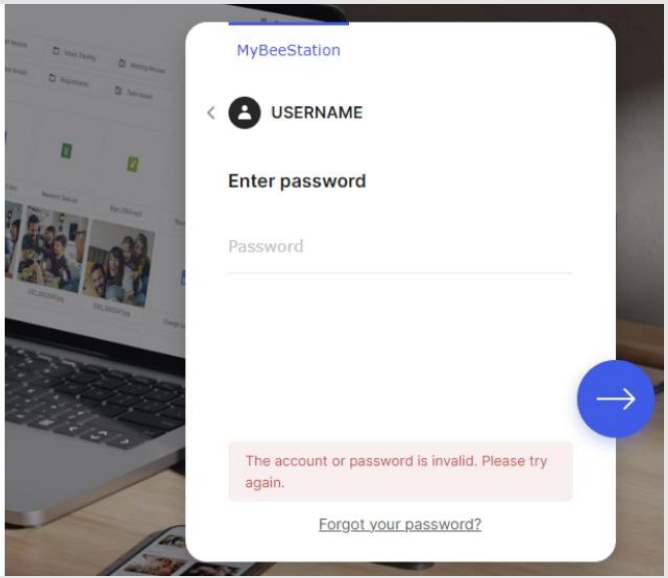
1. 尋找入口
2. 了解過程
3. 發現漏洞
4. Exploit

Improper Encoding of Output

1. 尋找入口
2. 了解過程
3. 發現漏洞
4. Exploit

最直覺的入口





Synology

Improper Encoding of Output

1. 尋找入口
2. 了解過程
3. 發現漏洞
4. Exploit

bpftrace 追蹤發生的事情

```
# bpftrace --unsafe /follow_syscall_activity.bt
Attaching 1 probe…

PID: 22515 CMD: NULL #[0]
PID: 22515 ENV:
PATH=/sbin:/bin:/usr/sbin:/usr/bin:/usr/syno/sbin:/usr/syno/bin:/usr/local/sbin
:/usr/local/bin
PID: 22515 ENV: SOCKET=/run/synoscgi.sock
PID: 22515 ENV: LD_PRELOAD=openhook.so
PID: 22515 ENV: CONTENT_LENGTH=1309
PID: 22515 ENV: REWRITE_APP=SYNO.SDS.Bee.Instance
PID: 22515 ENV: SCRIPT_FILENAME=/usr/syno/synoman/webapi/entry.cgi
PID: 22515 ENV: SCRIPT_NAME=/webapi/entry.cgi
PID: 22515 ENV: REQUEST_METHOD=POST
PID: 22515 ENV: REQUEST_URI=/webapi/entry.cgi?api=SYNO.BEE.API.Auth
PID: 22515 ENV: QUERY_STRING=api=SYNO.BEE.API.Auth
PID: 22515 ENV: CONTENT_TYPE=application/x-www-form-urlencoded; charset=UTF-8
PID: 22515 ENV: DOCUMENT_URI=/webapi/entry.cgi
```

Improper Encoding of Output

1. 尋找入口
2. 了解過程
3. 發現漏洞
4. Exploit

登入前 / 後會做其他事情

```
PID: 22691 CMD: /usr/syno/plugin/weblogin/synocgi-plugin-weblogin --post #[2]
PID: 22691 ENV:
PATH=/sbin:/bin:/usr/sbin:/usr/bin:/usr/syno/sbin:/usr/syno/bin:/usr/local/sbin
:/usr/local/bin
PID: 22691 ENV: USER=USERNAME
PID: 22691 ENV: TYPE=passwd
PID: 22691 ENV: SESSION=webui
PID: 22691 ENV: API_VERSION=7
PID: 22691 ENV: IS_KNOWN_DEVICE=no
PID: 22691 ENV: IP=192.168.50.186
PID: 22691 ENV: AGENT=Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0 Safari/537.36
PID: 22691 ENV: STATUS=fail
PID: 22691 ENV: RESULT=-2
PID: 22691 ENV:
SYNO_PLUGIN_ARGS=/run/synoplugind//tmp/env.22249.dd150dfd-ee00-4578-bcb3-f52ed0
f21e12 #[3]
PID: 22691 ENV: SYNO_PLUGIN_UUID=dd150dfd-ee00-4578-bcb3-f52ed0f21e12
PID: 22691 CMDL: /usr/syno/plugin/weblogin/synocgi-plugin-weblogin
PID: 22691 CMDL: --post
```


Synology

Improper Encoding of Output

1. 尋找入口
2. 了解過程
3. 發現漏洞
4. Exploit

環境變數有使用者名稱

```
PID: 22691 CMD: /usr/syno/plugin/weblogin/synocgi-plugin-weblogin --post #[2]
PID: 22691 ENV:
PATH=/sbin:/bin:/usr/sbin:/usr/bin:/usr/syno/sbin:/usr/syno/bin:/usr/local/sbin
:/usr/local/bin
PID: 22691 ENV: USER=USERNAME
PID: 22691 ENV: TYPE=passwd
PID: 22691 ENV: SESSION=webui
PID: 22691 ENV: API_VERSION=7
PID: 22691 ENV: IS_KNOWN_DEVICE=no
PID: 22691 ENV: IP=192.168.50.186
PID: 22691 ENV: AGENT=Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0 Safari/537.36
PID: 22691 ENV: STATUS=fail
PID: 22691 ENV: RESULT=-2
PID: 22691 ENV:
SYNO_PLUGIN_ARGS=/run/synoplugind//tmp/env.22249.dd150dfd-ee00-4578-bcb3-f52ed0
f21e12 #[3]
PID: 22691 ENV: SYNO_PLUGIN_UUID=dd150dfd-ee00-4578-bcb3-f52ed0f21e12
PID: 22691 CMDL: /usr/syno/plugin/weblogin/synocgi-plugin-weblogin
PID: 22691 CMDL: --post
```


Synology

Improper Encoding of Output

1. 尋找入口
2. 了解過程
3. 發現漏洞
4. Exploit

環境變數有暫存檔路徑

```
PID: 22691 CMD: /usr/syno/plugin/weblogin/synocgi-plugin-weblogin --post #[2]
PID: 22691 ENV:
PATH=/sbin:/bin:/usr/sbin:/usr/bin:/usr/syno/sbin:/usr/syno/bin:/usr/local/sbin
:/usr/local/bin
PID: 22691 ENV: USER=USERNAME
PID: 22691 ENV: TYPE=passwd
PID: 22691 ENV: SESSION=webui
PID: 22691 ENV: API_VERSION=7
PID: 22691 ENV: IS_KNOWN_DEVICE=no
PID: 22691 ENV: IP=192.168.50.186
PID: 22691 ENV: AGENT=Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0 Safari/537.36
PID: 22691 ENV: STATUS=fail
PID: 22691 ENV: RESULT=-2
PID: 22691 ENV:
SYNO_PLUGIN_ARGS=/run/synoplugind//tmp/env.22249.dd150dfd-ee00-4578-bcb3-f52ed0
f21e12 #[3]
PID: 22691 ENV: SYNO_PLUGIN_UUID=dd150dfd-ee00-4578-bcb3-f52ed0f21e12
PID: 22691 CMDL: /usr/syno/plugin/weblogin/synocgi-plugin-weblogin
PID: 22691 CMDL: --post
```


Synology

Improper Encoding of Output

1. 尋找入口
2. 了解過程
3. 發現漏洞
4. Exploit

暫存檔內容

```
USER=USERNAME
TYPE=passwd
SESSION=webui
API_VERSION=7
IS_KNOWN_DEVICE=no
IP=192.168.50.186
AGENT=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/128.0.0.0 Safari/537.36
STATUS=fail
RESULT=-2
```

Improper Encoding of Output

1. 尋找入口
2. 了解過程
3. 發現漏洞
4. Exploit

有種可以 injection 的感覺

```
▼ dsmForm: Object
    OTPcode: ""
    SSOToken: ""
    password: ""
    username: "USERNAME\nNEXTLINE"
```

```
USER=PLUGIN_VALUE_START
USERNAME
NEXTLINE
PLUGIN_VALUE_END
TYPE=passwd
SESSION=webui
API_VERSION=7
IS_KNOWN_DEVICE=no
IP=192.168.50.186
AGENT=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/128.0.0.0 Safari/537.36
STATUS=fail
RESULT=-2
```


Synology

Improper Encoding of Output

1. 尋找入口
2. 了解過程
3. 發現漏洞
4. Exploit

戳戳看

```
USER=PLUGIN_VALUE_START
USERNAME
PLUGIN_VALUE_END
NEWVAR=PLUGIN_VALUE_START
TEST
PLUGIN_VALUE_END
TYPE=passwd
SESSION=webui
API_VERSION=7
IS_KNOWN_DEVICE=no
IP=192.168.50.186
AGENT=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/128.0.0.0 Safari/537.36
STATUS=fail
RESULT=-2
```

Improper Encoding of Output

1. 尋找入口
2. 了解過程
3. 發現漏洞
4. Exploit

Bingo!

```
Args=[USER=USERNAME,NEWVAR=TEST,TYPE=passwd,SESSION=webui,API_VERSION=7,IS_KNOW
N_DEVICE=no,IP=192.168.50.186,AGENT=Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0
Safari/537.36,STATUS=fail,RESULT=-2]
```

Improper Encoding of Output

1. 尋找入口
2. 了解過程
3. 發現漏洞
4. Exploit

- Write to arbitrary file
  - `ld` related environ variables
- Understand cron daemon
  - Ignore malformed lines

Improper Encoding of Output

1. 尋找入口
2. 了解過程
3. 發現漏洞
4. Exploit

- Write to arbitrary file
  - `ld` related environ variables
    - LD_PRELOAD
    - LD_DEBUG
    - LD_DEBUG_OUTPUT
- Understand cron daemon
  - Ignore malformed lines

Improper Encoding of Output

1. 尋找入口
2. 了解過程
3. 發現漏洞
4. Exploit

- Write to arbitrary file
  - `ld` related environ variables
- Understand cron daemon
  - Ignore malformed lines

Improper Encoding of Output

關鍵疏漏

- 過度信任輸入的資料

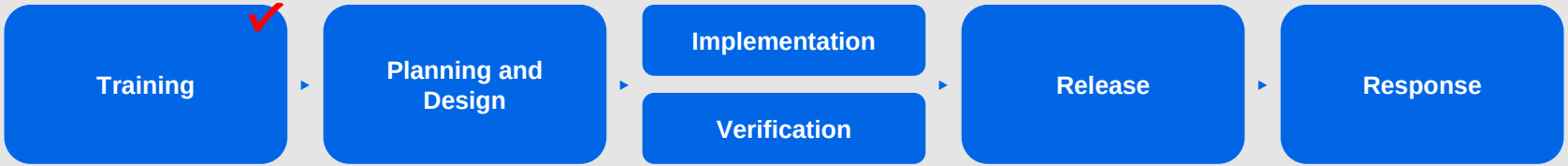
修復方式

- 輸出環境變數前先做編碼

Improper Encoding of Output

改進方式

- Internal Training
  - Newbie training
  - Regular sharing talk



Synology

總結

Synology

Summary

- 想提昇整體安全性
  - SAST
    - Coverity 需要花時間與人力 fine-tune
  - Toolchain hardening flag
    - Full RELRO
  - Memory-safe language
    - Rust
- 但 internal training 仍然不能少

Q & A

pohsingwu@synology.com

Synology