HomeAutomation 3.3.2 Open Redirect

2019.12.31			
Credit: **LiquidWorm (https://cxsecurity.com/author/LiquidWorm/1/)**			
Risk: **Medium**	Local: **No**	Remote: **Yes**	
CVE: **N/A**	CWE: **CWE-601 (https://cxsecurity.com/cwe/CWE-601)**		

```
HomeAutomation v3.3.2 Open Redirect


Vendor: Tom Rosenback and Daniel Malmgren
Product web page: http://karpero.mine.nu/ha/
Affected version: 3.3.2

Summary: HomeAutomation is an open-source web interface and scheduling solution.
It was initially made for use with the Telldus TellStick, but is now based on a
plugin system and except for Tellstick it also comes with support for Crestron,
OWFS and Z-Wave (using OpenZWave). It controls your devices (switches, dimmers,
etc.) based on an advanced scheduling system, taking into account things like
measurements from various sensors. With the houseplan view you can get a simple
overview of the status of your devices at their location in your house.

Desc: Input passed via the 'redirect' GET parameter in 'api.php' script is not
properly verified before being used to redirect users. This can be exploited to
redirect a user to an arbitrary website e.g. when a user clicks a specially crafted
link to the affected script hosted on a trusted domain.

==========================================================================
/api.php:
---------

80: if(file_exists(HA_ROOT_PATH."/api/".$_GET["do"].".php")) {
81:         $redirect = getFormVariable("redirect", "");
82:
83:         include(HA_ROOT_PATH."/api/".$_GET["do"].".php");
84:         $output = getFormVariable("output", "text");
85:
86:         if($redirect != "") {
87:                 redirectTo($redirect);
88:         } else {
89:                 echo $result;
90:         }
91: }

====================

/functions.php:
---------------

2252: function redirectTo($url, $statusCode = 303) {
2253:         if($url !== "") {
2254:                 SaveLog("Redirecting to ".$url, false, "redirects");
2255:                 header('Location: ' . $url, true, $statusCode);
2256:         die();
2257:         }
2258: }

==========================================================================
```

```
Tested on: Apache/2.4.41 (centos) OpenSSL/1.0.2k-fips
           Apache/2.4.29 (Ubuntu)
           PHP/7.4.0RC4
           PHP/7.3.11
           PHP 7.2.24-0ubuntu0.18.04.1


Vulnerability discovered by Gjoko 'LiquidWorm' Krstic
                            @zeroscience


Advisory ID: ZSL-2019-5559
Advisory URL: https://www.zeroscience.mk/en/vulnerabilities/ZSL-2019-5559.php


06.11.2019

--


http://localhost/homeautomation_v3_3_2/api.php?do=groups/toggle&groupid=1&status=1&redirect=https://zeroscience.mk
```

See this note in RAW Version (https://cxsecurity.com/ascii/WLB-2019120132)

Tv

Lul

Vote for this issue: 0 0

50% 50%

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)

Copyright **2022**, cxsecurity.com