HomeAutomation v3.3.2 CSRF Remote Command Execution (PHP Reverse Shell) PoC

Title: HomeAutomation v3.3.2 CSRF Remote Command Execution (PHP Reverse Shell) PoC
Advisory ID: ZSL-2019-5560
Type: Local/Remote
Impact: System Acces, DoS
Risk: (4/5)
Release Date: 29.12.2019

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.

Description

The application suffers from an authenticated OS command execution vulnerability using custom command v0.1 plugin. This can be exploited with CSRF vulnerability to execute arbitrary shell commands as the web user via the 'set_command_on' and 'set_command_off' POST parameters in '/system/systemplugins/customcommand/customcommand.plugin.php' by using an unsanitized PHP exec() function.

Vendor

Tom Rosenback and Daniel Malmgren - http://karpero.mine.nu/ha/

Affected Version

3.3.2

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

Vendor Status

[06.11.2019] Vulnerability discovered.
[07.11.2019] Vendor contacted.
[29.11.2019] No response from the vendor.
[30.11.2019] Vendor contacted.
[28.12.2019] No response from the vendor.
[29.12.2019] Public security advisory released.

PoC

homeautomation_rce.txt

Credits

Vulnerability discovered by Gjoko Krstic - <gjoko@zeroscience.mk>

References

[1] https://www.exploit-db.com/exploits/47809
[2] https://packetstormsecurity.com/files/155794/HomeAutomation-3.3.2-CSRF-Code-Execution.html
[3] https://cxsecurity.com/issue/WLB-2019120140
[4] https://exchange.xforce.ibmcloud.com/vulnerabilities/173659
[5] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-22000
[6] https://nvd.nist.gov/vuln/detail/CVE-2020-22000

Changelog

[29.12.2019] - Initial release
[24.01.2020] - Added reference [1], [2], [3] and [4]
[19.06.2021] - Added reference [5] and [6]

Contact

Zero Science Lab

Web: http://www.zeroscience.mk
e-mail: lab@zeroscience.mk

- **Profiles**

-