- Home
- Vulnerabilities!
- Blog
- Services
- About
- Contact

🇬🇧 🇲🇰

Smartwares HOME easy v1.0.9 Database Backup Information Disclosure Exploit

Title: Smartwares HOME easy v1.0.9 Database Backup Information Disclosure Exploit
Advisory ID: ZSL-2019-5541
Type: Local/Remote
Impact: Exposure of System Information, Exposure of Sensitive Information, Security Bypass
Risk: (4/5)
Release Date: 05.11.2019

Summary

Home Easy/Smartwares are a range of products designed to remotely control your home using wireless technology. Home Easy/Smartwares is very simple to set up and allows you to operate your electrical equipment like lighting, appliances, heating etc.

Description

The home automation solution is vulnerable to unauthenticated database backup download and information disclosure vulnerability. This can enable the attacker to disclose sensitive and clear-text information resulting in authentication bypass, session hijacking and full system control.

Vendor

Smartwares - https://www.smartwares.eu

Affected Version

<=1.0.9

Tested On

Boa/0.94.13

Vendor Status

[30.09.2019] Vulnerability discovered.
[01.10.2019] Vendor contacted.
[04.11.2019] No response from the vendor.
[05.11.2019] Public security advisory released.

PoC

homeeasy_backup.sh

Credits

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

References

[1] https://www.exploit-db.com/exploits/47596
[2] https://exchange.xforce.ibmcloud.com/vulnerabilities/171051
[3] https://packetstormsecurity.com/files/155177
[4] https://cve.mitre.org/cgi-bin/cvename.cgi?name=2020-21997
[5] https://nvd.nist.gov/vuln/detail/CVE-2020-21997

Changelog

[05.11.2019] - Initial release
[11.11.2019] - Added reference [1], [2] and [3]
[19.06.2021] - Added reference [4] and [5]

Contact

Zero Science Lab

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

- ## Rete mirabilia

- ## We Suggest

- ## Profiles