MyDomoAtHome (MDAH) REST API Domoticz ISS Gateway 0.2.40 Information Disclosure

Title: MyDomoAtHome (MDAH) REST API Domoticz ISS Gateway 0.2.40 Information Disclosure
Advisory ID: ZSL-2019-5555
Type: Local/Remote
Impact: Exposure of System Information, Exposure of Sensitive Information, Security Bypass
Risk: (4/5)
Release Date: 29.12.2019

Summary

REST Gateway between Domoticz and Imperihome ISS. Domoticz is a home automation system with a pretty wide library of supported devices, ranging from weather stations to smoke detectors to remote controls, and a large number of additional third-party integrations are documented on the project's website. It is designed with an HTML5 frontend, making it accessible from desktop browsers and most modern smartphones, and is lightweight, running on many low-power devices like the Raspberry Pi.

Description

MyDomoAtHome REST API is affected by an information disclosure vulnerability due to improper access control enforcement. An unauthenticated remote attacker can exploit this, via a specially crafted request to gain access to sensitive information.

Vendor

Emmanuel - https://github.com/empierre/MyDomoAtHome

Affected Version

0.2.40

Tested On

NodeJS: 10.15.0, 8.15.1, 8.15.0, 8.11.1, 8.9.4, 4.8.7, 4.2.2
Webmanager/Engine: EJS
Renderer: Express

Vendor Status

N/A

PoC

domoticz_info.txt

Credits

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

References

[1] https://www.exploit-db.com/exploits/47824
[2] https://packetstormsecurity.com/files/155787
[3] https://cxsecurity.com/issue/WLB-2020010007
[4] https://exchange.xforce.ibmcloud.com/vulnerabilities/173700
[5] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-21990
[6] https://nvd.nist.gov/vuln/detail/CVE-2020-21990
[7] https://www.tenable.com/cve/CVE-2020-21990

Changelog

[29.12.2019] - Initial release
[24.01.2020] - Added reference [1], [2], [3] and [4]
[19.06.2021] - Added reference [5], [6] and [7]

Contact

Zero Science Lab

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

- **Rete mirabilia**
- **We Suggest**
- **Profiles**

- Site Meter