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

AVE DOMINAplus <=1.10.x Credentials Disclosure Exploit

Title: AVE DOMINAplus <=1.10.x Credentials Disclosure Exploit
Advisory ID: ZSL-2019-5550
Type: Local/Remote
Impact: System Access, DoS, Security Bypass
Risk: (5/5)
Release Date: 27.12.2019

Summary

DOMINAplus - Sistema Domotica Avanzato. Advanced Home Automation System. Designed to revolutionize your concept of living. DOMINA plus is the AVE home automation proposal that makes houses safer, more welcoming and optimized. In fact, our home automation system introduces cutting-edge technologies, designed to improve people's lifestyle. DOMINA plus increases comfort, the level of safety and security and offers advanced supervision tools in order to learn how to evaluate and reduce consumption through various solutions dedicated to energy saving.

Description

The application suffers from clear-text credentials disclosure vulnerability that allows an unauthenticated attacker to issue a request to an unprotected directory that hosts an XML file '/xml/authClients.xml' and obtain administrative login information that allows for a successful authentication bypass attack.

Vendor

AVE S.p.A. - https://www.ave.it

Affected Version

Web Server Code 53AB-WBS - 1.10.62
Touch Screen Code TS01 - 1.0.65
Touch Screen Code TS03x-V | TS04X-V - 1.10.45a
Touch Screen Code TS05 - 1.10.36
Models: 53AB-WBS
TS01
TS03V
TS04X-V
TS05N-V
App version: 1.10.77
App version: 1.10.65
App version: 1.10.64
App version: 1.10.62
App version: 1.10.60
App version: 1.10.52
App version: 1.10.52A
App version: 1.10.49
App version: 1.10.46
App version: 1.10.45
App version: 1.10.44
App version: 1.10.35
App version: 1.10.25
App version: 1.10.22
App version: 1.10.11
App version: 1.8.4
App version: TS1-1.0.65
App version: TS1-1.0.62
App version: TS1-1.0.44
App version: TS1-1.0.10
App version: TS1-1.0.9

Tested On

GNU/Linux 4.1.19-armv7-x7
GNU/Linux 3.8.13-bone50/bone71.1/bone86
Apache/2.4.7 (Ubuntu)
Apache/2.2.22 (Debian)
PHP/5.5.9-1ubuntu4.23
PHP/5.4.41-0+deb7u1
PHP/5.4.36-0+deb7u3

Vendor Status

[06.10.2019] Vulnerability discovered.
[14.10.2019] Vendor contacted.
[20.10.2019] No response from the vendor.
[21.10.2019] Vendor contacted.
[26.12.2019] No response from the vendor.
[27.12.2019] Public security advisory released.

PoC

dominaplus_pwd.py

Credits

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

References

[1] https://packetstormsecurity.com/files/155763
[2] https://cxsecurity.com/issue/WLB-2019120113
[3] https://www.exploit-db.com/exploits/47819
[4] https://exchange.xforce.ibmcloud.com/vulnerabilities/173620
[5] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-21994
[6] https://nvd.nist.gov/vuln/detail/CVE-2020-21994
[7] https://www.tenable.com/cve/CVE-2020-21994

Changelog

[27.12.2019] - Initial release
[29.12.2019] - Added reference [1] and [2]
[24.01.2020] - Added reference [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