Inim Electronics Smartliving SmartLAN/G/SI <=6.x Unauthenticated SSRF

Title: Inim Electronics Smartliving SmartLAN/G/SI <=6.x Unauthenticated SSRF
Advisory ID: ZSL-2019-5545
Type: Local/Remote
Impact: Exposure of System Information
Risk: (3/5)
Release Date: 09.12.2019

Summary

SmartLiving anti-intrusion control panel and security system provides important features rarely found in residential, commercial or industrial application systems of its kind. This optimized-performance control panel provides first-rate features such as: graphic display, text-to-speech, voice notifier, flexible hardware, end-to-end voice transmission (voice-on-bus), IP connectivity.

SMARTLAN/SI: The system-on-chip platform used in the SmartLAN/SI accessory board provides point-to-point networking capability and fast connectivity to the Internet. Therefore, it is possible to set up a remote connection and program or control the system via the SmartLeague software application. In effect, the SmartLAN/SI board grants the same level of access to the system as a local RS232 connection.

SMARTLAN/G: The SmartLAN/G board operates in the same way as the SmartLAN/SI but in addition provides advanced remote-access and communication functions. The SmartLAN/G board is capable of sending event-related e-mails automatically. Each e-mail can be associated with a subject, an attachment and a text message. The attachment can be of any kind and is saved to an SD card. The message text can contain direct links to domains or IP addressable devices, such as a security cameras. In addition to e-mails, the SmartLAN/G board offers users global access to their control panels via any Internet browser accessed through a PC, PDA or Smartphone. In fact, the SmartLAN/G has an integrated web-server capable of distinguishing the means of connection and as a result provides an appropriate web-page for the tool in use. Smartphones can control the system in much the same way as a household keypad, from inside the house or from any part of the world.

Description

Unauthenticated Server-Side Request Forgery (SSRF) vulnerability exists in the SmartLiving SmartLAN within the GetImage functionality. The application parses user supplied data in the GET parameter 'host' to construct an image request to the service through onvif.cgi. Since no validation is carried out on the parameter, an attacker can specify an external domain and force the application to make an HTTP request to an arbitrary destination host. This can be used by an external attacker for example to bypass firewalls and initiate a service and network enumeration on the internal network through the affected application.

Vendor

INIM Electronics s.r.l. - https://www.inim.biz

Affected Version

<=6.x
SmartLiving 505
SmartLiving 515
SmartLiving 1050, SmartLiving 1050/G3
SmartLiving 10100L, SmartLiving10100L/G3

Tested On

GNU/Linux 3.2.1 armv5tejl
Boa/0.94.14rc21
BusyBox v1.20.2

Vendor Status

[06.09.2019] Vulnerability discovered.
[10.09.2019] Vendor contacted.
[10.10.2019] No response from the vendor.
[11.10.2019] Vendor contacted.
[29.11.2019] No response from the vendor.
[30.11.2019] Vendor contacted.
[08.12.2019] No response from the vendor.
[09.12.2019] Public security advisory released.

PoC

smartlan_ssrf.txt

Credits

Vulnerability discovered by Sipke Mellema - <sipke@zeroscience.mk>

References

[1] https://www.exploit-db.com/exploits/47764
[2] https://packetstormsecurity.com/files/155617
[3] https://exchange.xforce.ibmcloud.com/vulnerabilities/172839
[4] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-22002
[5] https://nvd.nist.gov/vuln/detail/CVE-2020-22002

Changelog

[09.12.2019] - Initial release
[12.12.2019] - 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**

-