AV-Comparatives & sigma star gmbh discovers security flaws in firmware used by 30+ popular TV brands, including Medion.

19th December 2017, Innsbruck, Austria – The independent security software tester AV-Comparatives joint up with sigma star gmbh and has decided to inform the general public of several critical vulnerabilities in Vestel firmware. Vestel is one of the largest manufacturer of electronics components in the world. Vestel components are used in more than 30 popular TV brands, including **Medion**.

Wikileaks tale turns into real life security threat

In March 2017 Wikileaks revealed news about the CIA and MI5 hacking Smart-TV's to spy on you. At AV-Comparatives we decided to fact check this story by performing a quick security check on the Medion smart-TV we use in our conference room.

To our surprise, we discovered real security issues and decided to ask sigma star gmbh (specialized in IOT) to analyze these issues in detail. sigma star gmbh confirmed the severity of these security issues. We informed Medion on April 4th 2017 about these flaws.

After warning Medion that the 90-day responsible disclosure period had passed, Medion formally responded:

RISK	Explanation	Medion confirmed	Solved
CVE 4.5	Remote Control commands not encrypted	Require investigation	No
CVE 4.6	Telemetry data not encrypted	Yes	New model's only
CVE 7.4	Third-party TV App's unencrypted download	Yes, but not responsible	No
CVE 7.9	Firmware update unencrypted download	Yes, but image is authenticated	New model's only
CVE 8.8	Remote Control arbitrary code execution[1]	Yes, risk downplayed	No
CVE 9.1	Possible remote-control port backdoor	Require investigation	No

We respect Medion's request to further investigate two critical vulnerabilities and will not disclose them for an additional period of 30 days. Although the formal response of Medion is correct and polite, the best outcome seems to be to provide a solution for newer models only. Existing owners are not offered a solution (firmware update) which solves those critical security vulnerabilities.

[1] 1. When on the same network, an attacker can send arbitrary TV remote control commands to the TV without authentication. This can for instance be used to remotely change the network configuration to establish a man-in-the-middle setup. 2.When on the same network, an attacker can request information from the TV, such as currently watched channel, volume settings, etc. without authentication. 3. When on the same network, an attacker can remotely invoke arbitrary shell commands with root privileges through a network service running on the TV.

Appeal to consumers to and smart TV-vendors

We advise consumers to ask the '*latent defects*' consumer protection clause to be applicable for firmware also when buying smart-TV's. A list of possible affected products can be obtained from Wikipedia: https://en.wikipedia.org/wiki/Vestel#Subsidiary_brands

Hopefully the affected smart-TV vendors will persuade Vestel to provide a firmware update for these severe security issues.

About AV-Comparatives

AV-Comparatives is an independent organization offering systematic testing that checks whether security software, such as PC/Mac-based antivirus products and mobile security solutions, lives up to its promises. AV-Comparatives is both ISO and EICAR certified and offers an unique real-world test environment for accurate antivirus testing and certification. AV-Comparatives offers freely accessible results to individuals, news organizations and scientific institutions.

About sigma star

We, the sigma star gmbh were founded by Thomas Dierl und Richard Weinberger in 2011 after they already worked together as independent contractors for ten years. With our currently 6 employees, we offer services around Linux consulting and development, security consulting and development and application development for hospitality with special demands. Our main principle is to supply always the best quality.

Contact information

Press contact: media@av-comparatives.org

Issues and Responses

Issue	CVSS Score	Additional info	Response from Medion
The TV sends plain text telemetry data to the manufacturer.	4.6	N/A	Telemetry data is very important for improving our product design. The telemetry data gathered from the field are analyzed to inform the design our future products. Security improvements are possible and we'll look into how we can incorporate your findings.
The 3rd party apps offered by the TV (e.g. YouTube player) are fetched from the vendors website without encryption or authentication.	7.4	N/A	3rd party applications enrich the user experience. In most cases, these applications are developed by 3rd parties unrelated to Vestel. Consequently, we do not always have control over how they are served. Some of these applications offer connections over HTTPS and whenever possible, they are preferred over the plain unencrypted versions.
Firmware updates are fetched through an unauthenticated and unencrypted FTP connection. A man-in-the-middle attacker can substitute arbitrary firmware binaries.	7.9	N/A	On our newer products, FTP update mechanism has been discontinued in favor of HTTPS. One mitigating factor here is that before the update procedures are performed on the TV, the downloaded firmware is authenticated.
When on the same network, an attacker can send arbitrary TV remote control commands to the TV without authentication. This can for instance be used to remotely change the network configuration to establish a man-in-the-middle setup.	8.8	N/A	To improve user experience, we offer several modes of interactivity. One of these modes is the ability to use handheld applications as remote controllers. It is possible to reverse engineer such applications and design new 3rd party applications that mimic our remote controller devices. Our TVs would respond as they would to a hardware remote controller. However, we think that the impact of misuse by such third-party applications would be limited to what can be done using a regular remote.
When on the same network, an attacker can request information from the TV, such as currently watched channel, volume settings, etc. without authentication.	4.5	For instance, the following unix shell line (where $ip holds the TVs ip address) retrieves an XML document	This functionality is provided so that rich handheld applications can be developed. However, we are investigating a possible redesign where we limit the information and services provided through the status port. Your observation that garbage information appended to the output of some of the commands seems to be a bug and we will investigate the cause.

		describing the currently selected channel from the TV: echo "GETINFO PROGRAM" | nc $ip 1986	
When on the same network, an attacker can remotely invoke arbitrary shell commands with root privileges through a network service running on the TV.	9.1	The following unix shell line starts a shell running as root user on the TV that can be accessed through telnet: echo "/bin/telnetd -l /bin/sh" | nc $ip 1986	We will investigate this vulnerability as part of the work done for point 4.2.

Detailed Issues Discovered by AV-C and sigma star

AV-C / sigma star: First contact via support form on website: **4th April 2017**

Medion: Response from Medion: Only automated response pointing to a chargeable phone number.

14th November 2017
Issues reported to Medion via web forum:

AV-C / sigma star

0) Summary
This report summarizes the most important aspects and results of the analysis of the MEDION LIFE X15016 smart TV as running firmware: application version V.3.3.8c and software upgrade version V.3.6.2j MED. As of today (October 17 2017) no further updates are available. The firmware was built on 2015-01-22 16:09 as reported by the user interface. While officially being branded as a MEDION television set, the TV electronics and firmware are actually manufactured by VESTEL, an electronics company based in Turkey that sells entertainment electronics under many different brand names (such as Telefunken) or licenses its technology to other manufacturers for re-branding (such as MEDION). VESTEL also provides services under the domains vstlsrv.com and portaltv.tv that are used by the TV firmware. As a result, any vulnerability discussed in this report may also exist in TVs from other brands and potentially other products that use VESTEL modules and share a common code base.

During analysis of the TV, it has been discovered that all relevant communications observed are unencrypted and unauthenticated, allowing for eavesdropping and man-in-the-middle attacks.

Furthermore, any computer that can reach the TV over the network can:
- Inject arbitrary remote-control events.
- Perform surveillance of the TVs usage.
- Force the TV to install a firmware image provided by an attacker.
- Execute arbitrary commands with root privileges on the TV.

Some of these problems are already known publicly but have been ignored by VESTEL. Those problems could possibly also exist on other products from other brands that use VESTEL modules. Apart from MEDION, this includes brands such as Telefunken, Panasonic, Philips, JVC or Toshiba. See APPENDIX B for a more exhaustive list.

Easy eavesdropping or exploitation of the TV is not only problematic in terms of privacy, but also in light of recent events involving internet connected "smart" devices ("Internet of Things") being incorporated into bot-nets used, for instance, for performing distributed denial of service attacks [6].

1) Overview of the vulnerabilities found on the TV

The TV sends plain text telemetry data to the manufacturer.

Overall CVSS Score 4.6

The 3rd party apps offered by the TV (e.g. YouTube player) are fetched from the vendors website without encryption or authentication.

Overall CVSS Score 7.4

Firmware updates are fetched through an unauthenticated and unencrypted FTP connection. A man-in-the-middle attacker can substitute arbitrary firmware binaries.

Overall CVSS Score 7.9

When on the same network, an attacker can send arbitrary TV remote control commands to the TV without authentication. This can for instance be used to remotely change the network configuration to establish a man-in-the-middle setup.

Overall CVSS Score 8.8

When on the same network, an attacker can request information from the TV, such as currently watched channel, volume settings, etc... without authentication.

Overall CVSS Score 4.5

When on the same network, an attacker can remotely invoke arbitrary shell commands with root privileges through a network service running on the TV.

Overall CVSS Score 9.1

2) Experimental setup

For all experiments, the TVs Ethernet port was connected to an Ethernet switch (NETGEAR FS608v3). No other ports on the TV were connected (except for power supply). An Arch Linux PC running dnsmasq 2.76 (DHCP & DNS server) was connected to the same switch. The DHCP server was configured to provide the IP address of the PC as default gateway and DNS server.

This way, the TV sends all traffic destined to hosts on the internet through the PC to utilize life capture and analysis using Wireshark 2.2.1. Iptables rules on the PC were used to explicitly control what traffic to forward to internet hosts. DNS requests from the TV were answered by the DNS server on the PC, which allowed for easy redirection of domain names to the IP address of the PC in experiments, so the TV connects directly to a service on the PC (e.g. FTP) instead of an internet host. This also allowed for testing the TVs responses to DNS spoofing.

3) Network Activity

Immediately after booting, the television set performs network auto configuration via DHCP. No attempts have been seen at IPv6 auto configuration (or any IPv6 traffic at all). The TV then proceeds to detect network connectivity by sending an ICMP request to 8.8.8.8 (google name server), fetches test data from the manufacturer website (such as http://portaltv.tv/assets/2kb.txt which contains 2048 times the letter 'x') and fetches network time via NTP. All communications observed during system boot are unencrypted and unauthenticated. Furthermore, the TV attempts to use a defunct IP location service. Since this communication is also in plain text, the API key used by the TV could be easily extracted. The entire request URL has been attached under [1]. The only encrypted communication encountered was a brief TLS session established with certs.opera.com on TCP port 443. This server hosts a certificate repository for the Opera web browser which provides both web browsing functionality of the TV, as well as HTML rendering of HbbTV content embedded in television broadcasts. This short TLS session was repeated throughout the operation of the TV and always followed by a plain text OCSP request.

3.1) Telemetry

During operation of the TV, plain text HTTP POST request to "vstlsrv.com" (a domain owned by VESTEL that points to an IPv4 address owned by Amazon) were occasionally observed.
Those requests posted telemetry data to "/InsertDB.aspx" including:

- The local IP address of the TV
- The name of the retailer that sold the TV ("ALDINORD")
- The particular VESTEL hardware installed in the TV ("MB90")
- The firmware version ("3.6.2.j")
- The MAC address of the Ethernet interface
- Presumably a region string ("de|at")
- Through what kind of TV tuner the TV signal is received ("Terrestrial")
- How the TV is connected to the internet ("Ethernet")
- The name and version of a software component installed on the TV ("Thorium", "02M-338_1.6S95M")
- Other, unknown integer identifiers

Because this telemetry data is transmitted in plain, an eavesdropper even outside the local network that the TV is connected to can gain information about the presence of the TV, firmware details and through which IP and MAC addresses the TV can be reached inside the network.

CVSS Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:X/RL:U/RC:X/CR:L/IR:X/AR:X/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:L/MI:N/MA:N

CVSS Base Score 5.3
Impact Subscore 1.4
Exploitability Subscore 3.9
CVSS Temporal Score 5.3
CVSS Environmental Score 4.6
Modified Impact Subscore 0.7
Overall CVSS Score 4.6

3.2) TV Web Browser

By default, the Web Browser on the TV fetches a landing page from "portaltv.tv", again provided by VESTEL and hosted by Amazon. All observed communications were unencrypted and unauthenticated, and are thus vulnerable for both eavesdropping and man-in-the-middle attacks. The TV offers to run "apps" which are basically HTML+JavaScript based web applications run on the TV. While some of the tested 3rd party applications (e.g. YouTube viewer) initiated TLS connections, the applications themselves were fetched through unencrypted, unauthenticated HTTP.

A man-in-the-middle attacker can intercept apps fetched from the server and provide substitutes that don't use TLS, thus allowing the attacker, for instance, to eavesdrop on login credentials or exchange information displayed.

CVSS Vector:
CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:X/RL:U/RC:X/CR:M/IR:M/AR:X/MAV:N/MAC:H/MPR:N/MUI:N/MS:U/MC:H/MI:H/MA:N

CVSS Base Score 7.4
Impact Subscore 5.2
Exploitability Subscore 2.2
CVSS Temporal Score 7.4
CVSS Environmental Score 7.4
Modified Impact Subscore 5.2
Overall CVSS Score 7.4

3.3) Firmware update

When requesting the TV to check for firmware updates, it connects to an FTP server on "vstlsrv.com" that hosts firmware images for different VESTEL products. The FTP server requests authentication through username and password, however the FTP connection itself is unencrypted, thus the username "17MB90" and password "vstl.1978" could be obtained by observing the login attempt made by the TV. Credentials of the VESTEL FTP server have been previously released on the internet [2][3]. VESTEL responded at least once around late 2014 or early 2015 by changing the credentials [3], thus ignoring the actual problem and permanently disabling firmware updates for devices with older firmware versions. Redirecting the DNS entry for vstlsrv.com causes the TV to connect to an FTP server running on the specified IP. Analysis of the firmware images from the FTP server suggests that they are not encrypted but obfuscated. It is not possible to say whether the images are authenticated.

A man-in-the-middle attacker can redirect connections to the VESTEL FTP server to an attacker controlled server and effectively cause the TV to install an arbitrary, attacker provided firmware image. This has to be considered a critical security vulnerability as an attacker can gain complete control over the software running on the TV. This is only possible if the firmware images are not authenticated.

CVSS Vector:
CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H/E/RL:U/RC:C/CR:H/IR:H/AR:L/MAV:N/MAC:H/MPR:N/MUI:R/MS:C/MC:H/MI:H/MA:H
CVSS Base Score 8.3
Impact Subscore 6.0
Exploitability Subscore 1.6
CVSS Temporal Score 7.9
CVSS Environmental Score 7.9
Modified Impact Subscore 6.0
Overall CVSS Score 7.9

4) Port Scan & Service Detection

A port scan on the TV revealed the following open TCP ports:

- 4661
- 4660
- 1986

4.1) Remote Control Port

The ports 4661 and 4660 are used by the MEDION Life Remote App for remote controlling the TV.

Reverse engineering of the app revealed that 4661 is used for transmitting touch pad events and 4660 for key presses on the virtual TV remote. TV remote keys are encoded as integers, transmitted as ASCII strings, followed by a line feed. For instance, "1048\n" co-responds to pressing the menu button.

See APPENDIX A for a complete key code mapping.

Since this service is again unencrypted and unauthenticated, any computer in the network can send key press commands to the TV. This is especially critical in combination with the vulnerable firmware updater mentioned in 3.3, since an attacker no longer has to be a man-in-the-middle. An attacker on the same network as the TV can send key commands to blindly change the network settings in the menu, so the TV uses the attacker IP as default gateway and then send a sequence of key presses that trigger the firmware update option in the menu.

CVSS Vector:
CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:H/E/RL:U/RC:C/CR:X/IR:X/AR:X/MAV:A/MAC:L/MPR:N/MUI:N/MS:C/MC:N/MI:H/MA:H
CVSS Base Score 9.3
Impact Subscore 5.8
Exploitability Subscore 2.8
CVSS Temporal Score 8.8
CVSS Environmental Score 8.8
Modified Impact Subscore 5.8
Overall CVSS Score 8.8

4.2) Status Port

Port 1986 is used by the remote app to request status information by sending plain text commands and retrieving XML responses including information such as:

- Current volume level of the TV
- TV channel being currently watched

Again, this service is unauthenticated and unencrypted, and allows any system on the same network to request information, giving rise to potential privacy violations as an attacker can query the currently watched TV channel and use publicly available channel listings to determine what is being watched on the TV at any given time.

For instance, the following unix shell line (where $ip holds the TVs ip address) retrieves an XML document describing the currently selected channel from the TV:

```
echo "GETINFO PROGRAM" | nc $ip 1986
```

It should be noted, that the XML strings returned by the TV were followed by garbled binary data of varying length and content, hinting at a missing null-terminator in the TV software. This could potentially be used to extract further information. When given malformed input (such as an HTTP request header) the port is still open, but the service stops responding, hinting at further issues in the command parser.

CVSS Vector:
CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E/RL:U/RC:C/CR:L/IR:X/AR:X/MAV:A/MAC:L/MPR:N/MUI:N/MS:U/MC:H/MI:N/MA:N
CVSS Base Score 6.5
Impact Subscore 3.6
Exploitability Subscore 2.8
CVSS Temporal Score 6.2
CVSS Environmental Score 4.5
Modified Impact Subscore 1.8
Overall CVSS Score 4.5

4.3) Possible Backdoor

When encountering a command it cannot interpret, the status service on port 1986 simply executes any given string in a shell with root privileges on the TV.
For instance, the following unix shell line (where $ip holds the TVs ip address and $dst is an arbitrary destination ip address) causes the TV to send a single ICMP echo request to an arbitrary destination:

```
echo "ping -c 1 $dst" | nc $ip 1986
```

The following unix shell line starts a shell running as root user on the TV that can be accessed through telnet:

```
echo "/bin/telnetd -l /bin/sh" | nc $ip 1986
```

This behavior is apparently also present in other TVs with VESTEL modules and has to some degree been publicly known since at least July 2016[4].

THIS IS A SEVERE VULNERABILITY. Any computer on the same network as the TV can execute arbitrary shell commands with root privileges.

CVSS Vector:
CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E/RL:U/RC:C/CR:M/IR:M/AR:M/MAV:A/MAC:L/MPR:N/MUI:N/MS:C/MC:H/MI:H/MA:H

CVSS Base Score 9.6
Impact Subscore 6.0
Exploitability Subscore 2.8
CVSS Temporal Score 9.1
CVSS Environmental Score 9.1
Modified Impact Subscore 6.0
Overall CVSS Score 9.1

5) References

[1] http://api.ipinfodb.com/v3/ip-city/?key=4214d26be2e51d2192682dc815486a8614fc982a0f18604036d80bf0d1a1...
[2] https://forum.digitalfernsehen.de/threads/medion-md-30465-42-led-backlight-tv-life%C2%AE-x17006.2763...See also screenshot website_1.png
[3] https://forum.digitalfernsehen.de/threads/telefunken-d49f283a3c-mb95-board.344736
See also screenshot website_2.png
[4] https://forum.digitalfernsehen.de/threads/medion-md-30465-42-led-backlight-tv-life%C2%AE-x17006.2763...
See also screenshot website_3.png
[5] https://en.wikipedia.org/wiki/Vestel
[6] https://en.wikipedia.org/wiki/Mirai_(malware)

APPENDIX A)

The television remote control app contains the following mapping of buttons to strings. The strings are sent to TCP port 4660 on the TV, followed by a new line:

BUTTON_HOME "1046"
BUTTON_POWER "1012"
BUTTON_POWER_NAV "1012"
BUTTON_POWER_PLAYER "1012"
BUTTON_POWER_PVM "1012"
BUTTON_POWER_GES_NAV "1012"
BUTTON_POWER_GES_PLAYER "1012"
BUTTON_POWER_GES_PVM "1012"
BUTTON_RECORD "1051"
BUTTON_PLAY "1025"
BUTTON_PAUSE "1049"
BUTTON_STOP "1024"
BUTTON_PREVIOUS "1034"
BUTTON_REWIND "1027"
BUTTON_FORWARD "1028"
BUTTON_NEXT "1255"
BUTTON_SCREEN "1011"
BUTTON_LANG "1015"
BUTTON_SUBTITLE "1031"
BUTTON_PRESETS "1014"
BUTTON_EPG "1047"
BUTTON_TEXT "1255"
BUTTON_FAV "1040"
BUTTON_3D "1040"
BUTTON_SLEEP "1042"
BUTTON_0 "1000"
BUTTON_1 "1001"
BUTTON_2 "1002"
BUTTON_3 "1003"
BUTTON_4 "1004"
BUTTON_5 "1005"
BUTTON_6 "1006"
BUTTON_7 "1007"
BUTTON_8 "1008"
BUTTON_9 "1009"
BUTTON_MENU "1048"
BUTTON_MUTE "1013"
BUTTON_UP "1020"
BUTTON_LEFT "1021"
BUTTON_OK "1053"
BUTTON_RIGHT "1022"
BUTTON_DOWN "1019"
BUTTON_VOL_UP "1016"
BUTTON_VOL_DOWN "1017"
BUTTON_VOL_UP_2 "1016"
BUTTON_VOL_DOWN_2 "1017"
BUTTON_PROG_UP "1032"
BUTTON_PROG_DOWN "1033"
BUTTON_BACK "1010"
BUTTON_EXIT "1037"
BUTTON_RED "1055"
BUTTON_GREEN "1054"

```
BUTTON_YELLOW "1050"
BUTTON_BLUE "1052"
BUTTON_INFO "1018"
BUTTON_MMEDIA "1057"
BUTTON_SOURCE "1056"
BUTTON_SWAP "1034"
BUTTON_CHAN "1045"
BUTTON_QMENU "1043"
KEYBOARD_BACKSPACE "8"
KEYBOARD_NEW_LINE "10"
```

It should be noted that decimal 8 (KEYBOARD_BACKSPACE) is actually the ASCII backspace character and decimal 10 (KEYBOARD_NEW_LINE) is the ASCII line feed character. The app internally also contains an explicit mapping of the values 48-57 to "48" to "57" (ASCII values for digits 0 to 9). Other ASCII characters are also encoded by printing their decimal value to a string.

APPENDIX B)

According to Wikipedia on the 2016-11-24[5], the following companies sell electronic devices using modules from VESTEL or sell re-branded VESTEL devices:

Subsidiary brands
Digihome, a consumer electronics brand
Electra, a UK white goods brand
Finlux, a Finnish consumer electronics brand
Graetz, a white goods brand sold in German-speaking countries
Innohit (Italian TV brand) is manufactured under license from the brand owner.
Isis, a UK TV and white goods brand
Celcus, a UK TV brand exclusively sold by Sainsbury's supermarkets
Luxor, a former Swedish brand previously owned by Nokia
MAXWELL, manufactures TV Sets, DVD players, and white goods (mainly refrigerators, air conditioners, cooking stoves, washing machines)
Regal, a Turkish brand also sold in Russia
SEG, a German brand also sold in Russia
Servis, a UK white goods brand
Sharp as Sharp Home Appliances Europe, Sharp Corporation (Japanese brand) white goods for Europe are manufactured under license from the brand owner. Rebadged flagship Servis models.
Techwood, a consumer electronics brand
Telefunken (German TV brand) is manufactured under license from the brand owner.
Vestfrost, a former Danish white goods brand purchased by Vestel
Waltham, a former UK brand purchased by Vestel
Kendo, manufactures TV sets and set top boxes
Acoustic Solutions, TV manufacturer
Walker, electronics for the marked in Ireland
GoGen, an East European brand of TV sets and other electronic products
New Pol
Nexon

Related brands
AKAI - for some countries, Vestel sets are branded AKAI.
CROWN - Vestel sells TV sets under the name CROWN.
Daewoo - some TV sets made by Vestel are marketed under the DAEWOO brand in some countries.
Dual - a German electronics brand. Some sets branded DUAL are made by Vestel.
Emerson - some Emerson sets were made by Vestel, for Europe, in some countries.
Ferguson - LCD TV sets branded Ferguson and marketed by a Polish company, are made by Vestel.
Funai - some Funai CRT sets were made by Vestel.
Gorenje - TV sets are made by Vestel.
Hitachi - Vestel is rebranding some of its TV sets as HITACHI, in some countries.
Horizon - low cost brand, usually LED TV's, marketed in Romania by NOD distribution, previous ASEsoft.
Hyundai - TV Sets, both TFT and CRT TV sets were manufactured by Vestel, for some countries
ITT and Schaub & Lorenz - some sets under these German brands are made by Vestel.
JVC - some JVC TV sets, both TFT and CRT, were manufactured by Vestel. Also, today, Vestel sells in some countries, LCD TV sets branded JVC.
LINSAR - independent British company that was established in 2006 were made by Vestel up until 2015. In 2016 Linsar was acquired by Tempo (Aust) Pty Ltd.
MEDION - German brand of consumer electronics. Many MEDION TV sets were and are manufactured by Vestel. Also, Tevion, Microstar, Lifetec brands are found on Vestel TV sets.
No.1 - Brand belonging to Carrefour. Some TV sets and budget home appliances under this brand, were made by Vestel.
Nordmende - some Vestel TV sets are marketed under Nordmende brand (with the permission from Thomson, today Technicolor).
Orion - some TV sets made by Vestel are branded Orion Electric, for some countries. Orion TV sets with Vestel chassis, were usually belonging to ORION Hungary, a Hungarian electronics manufacturer.

Palladium - a brand of TV Sets. Some Palladium sets were made by Vestel.
Panasonic - some LED TV sets from Panasonic, such as the A300, CX350 and CX400, are made by Vestel, these are mainly entry level/budget, HD, FullHD and some low cost (cx400 series) Ultra HD 4K models.
Philips - some LED TV from PHILIPS (like 32PFL3008) are made by Vestel, mainly entry level models.
Polaroid - LCD TV sets from Polaroid, in Europe, are made by Vestel.
RCA - in Europe, some Vestel sets were sold under RCA name.
Selecline - brand belonging to Auchan, France, used for TV sets and other electrical consumer products sold by Auchan.
Saba - some Vestel Sets are marketed under the name SABA (permission from Thomson, today Technicolor).
SANYO - some TV sets made by Vestel were sold under the brand SANYO in some countries.
Qilive - brand belonging to Auchan, France, used for TV sets and other electrical consumer products sold by Auchan.
Technika - brand owned by Tesco. Some older models used Vestel chassis.
TELETECH - low cost electronics brand, belonging to ALTEX Romania.
TELETECH televisions are made by Vestel
Tesla - a brand from Czechoslovakia. In countries that once formed Czechoslovakia, LCD TV sets made by Vestel were marketed under the name TESLA, but also ORAVA in some cases.
Toshiba - many sets named Toshiba are manufactured by Vestel, for European market.
Universum - German brand belonging to Quelle. Some Universum sets were manufactured by Vestel, both TFT and CRT.
Videoton - Hungarian electronics company. In Hungary, there were available Videoton LCD TV sets. The TV sets were made by Vestel, and usually sold in Hungary.
Watson Brand belonging to METRO GROUP - many Watson TV sets were made by Vestel.
WESTWOOD - low cost electronics brand belonging to DOMO Romania.
WESTWOOD televisions are made by Vestel.

Response from Medion 26.11.2017, 13:53

Re: Vulnerabilities in Smart TV

Hallo Herr XXX,

zu dem weitergeleiteten Protokoll erreichte uns folgende Rückmeldung:

Thank you for your analysis report. In matters of our TV product design, we welcome external input and we will be happy to work with you to understand the issues better. We take security of our products seriously and we strive to improve it with every new product line. Some of the vulnerabilities discovered by your analysis were already mitigated in our newer products.

We'd like to respond to some of your comments in the report. Here's our comments regarding the points that were made in the report:

3.1) Telemetry. The TV sends plain text telemetry data to the manufacturer.

Telemetry data is very important for improving our product design. The telemetry data gathered from the field are analyzed to inform the design our future products. Security improvements are possible and we'll look into how we can incorporate your findings.

3.2) TV Web Browser. The 3rd party apps offered by the TV (e.g. youtube player) are fetched from the vendors website without encryption or authentication.

3rd party applications enrich the user experience. In most cases, these applications are developed by 3rd parties unrelated to Vestel. Consequently, we do not always have control over how they are served. Some of these applications offer connections over HTTPS and whenever possible, they are preferred over the plain unencrypted versions.

3.3) Firmware update. Firmware updates are fetched through an unauthenticated and unencrypted FTP connection. A man-in-the-middle attacker can substitute arbitrary firmware binaries. On our newer products, FTP update mechanism has been discontinued in favor of HTTPS. One mitigating factor here is that before the update procedures are performed on the TV, the downloaded firmware is authenticated.

4.1) Remote Control Port. When on the same network, an attacker can send arbitrary TV remote control commands to the TV without authentication. This can for instance be used to remotely change the network configuration to establish a man-in-the-middle setup.

To improve user experience, we offer several modes of interactivity. One of these modes is the ability to use handheld applications as remote controllers. It is possible to reverse engineer such applications and design new 3rd party applications that mimic our remote controller devices. Our TVs would respond as they would to a hardware remote controller. However, we think that the impact of misuse by such third-party applications would be limited to what can be done using a regular remote.

4.2) Status Port. When on the same network, an attacker can request information from the TV, such as currently watched channel, volume settings, etc. without authentication. This functionality is provided so that rich handheld applications can be developed. However, we are investigating a possible redesign where we limit the information and services provided through the status port. Your observation that garbage information appended to the output of some of the commands seems to be a bug and we will investigate the cause.

4.3) Possible Backdoor. When on the same network, an attacker can remotely invoke arbitrary shell commands with root privileges through a network service running on the TV.

We will investigate this vulnerability as part of the work done for point 4.2.

Bei weiteren Fragen stehen wir selbstverständlich gern zur Verfügung.

Mit freundlichen Grüßen

snooker