Malwarebytes | Labs

NEWS, PRIVACY

LG TV flaws could let attackers listen in, even in standby mode

by Pieter Arntz | September 7, 2026



Add as a preferred source on Google

Smart TVs are internet-connected computers with microphones, app stores, advertising systems, and access to the same home networks used by your family's phones, laptops, printers, and smart-home devices.

In the past, we reported on Samsung settling a lawsuit with the Texas Attorney General over how its smart TVs collect and monetize viewing data using Automated Content Recognition (ACR).

ACR technology samples what appears on or is heard through a TV, creates a digital fingerprint, and compares that fingerprint against a reference database. It can be used to

security researchers, has examined several LG TV models. The team says it's found extensive device and network discovery, ACR tracking, and security weaknesses that could increase the consequences if a television were compromised.

Some findings concern LG's intended product behavior, while others rely on vulnerabilities that researchers say are still being disclosed responsibly. But the broader lesson is clear: A smart TV deserves the same privacy and security consideration as any other internet-connected computer.

According to Gamers Nexus, packet captures and firmware analysis showed the tested LG TVs identifying devices on the local network, such as phones, PCs, printers, switches, and smart-home hardware. The investigation also says the TVs collected nearby Wi-Fi network names, signal information, and device-related identifiers.

This network information could help build a picture of the other devices in a household. Combined with ACR data, advertising IDs, and other information, it could support detailed profiles of what people watch and the devices they use.

The researchers also demonstrated how a compromised TV could capture audio through its microphone, including when the TV appeared to be off. They even showed how the TV stored audio when it was unplugged from the internet and retrieved it after the connection was restored.

The researchers also reported remote-code-execution vulnerabilities to LG. They have not disclosed full details while the responsible disclosure process is ongoing.

A compromised television could be more than a privacy issue. It might provide an attacker with a foothold on a home or business network, access to audio, or a route to probe other devices.

How to stay safe

The concerns are not limited to one brand. Smart TVs sit at the intersection of entertainment, advertising, and the home network. Treating them as security-sensitive devices—and demanding clear, meaningful privacy choices—is increasingly part of staying safe at home.

There is no need to panic, but owners can take a few practical steps to limit what their TV collects and what it can access:

- **Install firmware updates** promptly, especially security updates. Check your model's support page and the TV's software-update settings.
- **Review the privacy controls** under Settings, Privacy & Terms, or User Agreements. Turn off ACR, viewing-information collection, personalized ads, voice recognition, and other features you don't need.

Malwarebytes | Labs

- **Use a separate IoT or guest network** for televisions, cameras, speakers, and other smart-home devices. This limits what a compromised device can reach on your main network.
- **Disable UPnP** on your router unless it is genuinely needed and avoid exposing TV services directly to the internet.

Our earlier guide to disabling ACR includes instructions for several popular TV brands.

Browse like no one's watching.

Malwarebytes Privacy VPN encrypts your connection and never logs what you do, so the next story you read doesn't have to feel personal. Try it free →

SHARE THIS ARTICLE

Add as a preferred source on Google

About the author



Pieter Arntz
Malware Intelligence Researcher

Was a Microsoft MVP in consumer security for 12 years running. Can speak four languages. Smells of rich mahogany and leather-bound books.

Malwarebytes | Labs

strip URLs, and publish your message.

What do you think?

26 Responses

 Upvote

 Funny

 Love

 Angry

 Sad

2 Comments Login ▾

G Join the discussion...

LOG IN WITH OR SIGN UP WITH DISQUS ?

Name

♡ Share Best Newest Oldest

B **Buddy**

2 days ago

How safe is it to have a FaceBook and/or Instagram account?

0 0 Reply



Pieter Arntz Mod → Buddy

2 days ago

Hi Buddy, That depends very much on how you use it. Be mindful of any information that you share and with whom.

0 0 Reply

Subscribe Privacy Do Not Sell My Data

Malwarebytes | Labs

BUGS



Microsoft fixes record 964 flaws, including 2 exploited zero-days

September 9, 2026

Microsoft's September 2026 Patch Tuesday fixes a record 964 vulnerabilities, including two actively exploited zero-days.

NEWS

Malwarebytes | Labs

Grindr settles HIV status data-sharing lawsuit for $35 million

September 8, 2026

Grindr has settled a UK lawsuit alleging that it shared sensitive user data, including HIV status, with advertising companies.

NEWS



MikroTik router flaws allow takeover without a password

September 8, 2026

Malwarebytes | Labs

Related articles



Grindr settles HIV status data-sharing lawsuit for $35 million

September 8, 2026

LG TV flaws could let attackers listen in, even in standby mode

September 7, 2026

153M+ driver's licenses for sale on new dark web platform

September 2, 2026

Sign up for our newsletter to get the latest cybersecurity news to your inbox

Email address

Sign Up

By submitting this form, you consent to Malwarebytes contacting you regarding products and services and using your personal data as described in our Terms of Service and Privacy Policy.

Malwarebytes - all-in-one cybersecurity protection always by your side.

Cybersecurity info you can't live without

Want to stay informed on the latest news in cybersecurity? Sign up for our newsletter and learn how to protect your computer from threats.

Email Address

Email Address

Sign Up

By submitting this form, you consent to Malwarebytes contacting you regarding products and services and using your personal data as described in our Terms of Service and Privacy Policy.

COMPUTER SECURITY

Rootkit Scanner

Trojan Scanner

Free Antivirus

Free Virus Scan

Premium protection

MOBILE SECURITY

GET IT ON Google Play

iOS Security and Spam Blocker

PRIVACY PROTECTION

Digital Footprint Scan

Dark Web Monitoring

Adware Removal

Ad Blocker

IDENTITY PROTECTION

Identity Monitoring & Alerts

Credit Monitoring & Reporting

Identity Recovery & Resolution

ID Theft Insurance

Personal Data Remover

Malwarebytes | Labs

Business Endpoint Security Solutions

Managed Service Provider (MSP) Program

LEARN ABOUT CYBERSECURITY

Blog

Social Engineering

Phishing

Ransomware

Malware

Antivirus

What is a VPN?

Doxxing

PARTNER WITH MALWAREBYTES

Computer Repair

Affiliates

Strategic Business Partnerships

Resellers

ADDRESS

One Albert Quay
2nd Floor
Cork T12 X8N6
Ireland

ABOUT MALWAREBYTES

Careers

News and Press

Vulnerability Disclosure

Report a False Positive

Territory Notice

Special Offers

WHY US

Malwarebytes vs. Bitdefender

Malwarebytes vs. McAfee

Malwarebytes vs. Norton

Malwarebytes vs. Microsoft Defender

GET HELP

Forums

Sign in to MyAccount

Help Center

English

Malwarebytes | Labs

Privacy

Terms of Service

Accessibility

© 2026 All Rights Reserved