

LG Smart TVs Vulnerable to Pre-Authentication Root Takeover via Local Network



Three vulnerabilities in LG webOS allow attackers on the same local network to gain root access to certain smart TV models without PIN or user interaction; LG has released a fix.

- Three vulnerabilities in LG webOS can be chained to enable pre-authentication root access from the local network
- Attack requires no PIN entry or user interaction from the TV owner
- Vulnerability affects specific LG smart TV models including 32LQ636BPSA and 27TQ600SW running webOS 7.5.7-25
- LG has issued a security fix according to SSD Secure Disclosure advisory published October 12
- Exploit requires attacker presence on the same local network as the vulnerable device

Vulnerability Overview

Security researchers have disclosed three vulnerabilities in LG's webOS operating system that can be exploited in combination to grant an attacker complete root access to certain smart television models. The attack vector requires the attacker to be present on the same local network as the target device but does not require any authentication credentials, PIN entry, or interaction from the device owner.

According to an advisory published by SSD Secure Disclosure on October 12, the vulnerability chain was successfully tested on two LG television models: the 32LQ636BPSA and the 27TQ600SW, both running webOS version 7.5.7-25 on their respective firmware. LG has acknowledged the security issues and issued a fix for affected devices.

Implications for Regulated Institutions

While consumer smart TVs may appear peripheral to core enterprise security, these devices are increasingly present in corporate environments including executive offices, conference rooms, and public-facing areas within regulated institutions. A compromised smart TV on the corporate network can serve as a foothold for lateral movement, network reconnaissance, or data exfiltration.

The **pre-authentication** nature of this vulnerability chain is particularly concerning, as it bypasses normal access controls entirely. An attacker who gains access to the local network—whether through physical presence, compromised Wi-Fi credentials, or other network vulnerabilities—can exploit these flaws without triggering authentication alerts or requiring social engineering.

Mitigation and Patch Management

Organizations should prioritize identifying all LG smart TV devices on their networks and ensuring firmware updates are applied promptly. The availability of a vendor-issued fix reduces the risk significantly, but only if deployed systematically across all affected devices.

What to do now

1. Conduct an inventory of all LG smart TV devices connected to corporate networks, including those in executive offices, conference rooms, and public areas
2. Apply the vendor-issued firmware update to all identified LG webOS devices running version 7.5.7-25 or earlier
3. Implement network segmentation to isolate smart TVs and other IoT devices from critical business systems and data networks
4. Review and restrict local network access controls, ensuring guest Wi-Fi and corporate networks are properly segregated
5. Update asset management databases to include all smart displays and IoT devices for ongoing vulnerability tracking

6. Establish a patch management process for non-traditional IT assets including smart TVs, displays, and conference room equipment