https://arstechnica.com/security/2012/12/how-an-internet-connected-samsung-tv-can-spill-your-deepest-secrets/

How an Internet-connected Samsung TV can spill your deepest secrets

Hack demonstrates the growing vulnerability of consumer devices.

Dan Goodin - 12/12/2012, 8:00 PM

f you use a Samsung "Smart TV" that's connected to the Internet, there's a good chance Luigi Auriemma can hack into the device and access files stored on connected USB drives.

The researcher with Malta-based security firm ReVuln says he has uncovered a vulnerability in most Samsung models that makes it easy for him to locate their IP address on the Internet. From there, he can remotely access the device and exercise the same control someone in the same room would have. That includes gaining root access and installing malicious software. The attack exploits bugs in features that allow end users to install Skype, Pandora, and other types of apps. The TVs can be controlled using smartphone and tablet apps and in some cases by voice commands.

"At this point the attacker has complete control over the device," he wrote in an e-mail to Ars. "So we are talking about applying custom firmwares, spying on the victim if camera and microphone are available, stealing any credential and account stored... on the device, using his own certificates when accessing https websites, and tracking any activity of the victim (movies, photos, music, and websites seen) and so on. You become the TV."

Auriemma declined to disclose technical details to prevent others from carrying out malicious attacks without paying for the research. ReVuln is primarily a research firm that discovers and sells zero-day exploits in a wide range of products.

It's not the first time Auriemma has hacked the Internet-facing controls of a Samsung TV. In April he disclosed a bug in a Samsung D6000 model belonging to his brother. It allowed him to send it into an endless restart mode that persisted even after unplugging the device and turning it back on. He said at the time he wouldn't be surprised if he could carry out more serious attacks against the device even when he didn't have access to the local network it was connected to.

Auriemma's research raises the possibility that owners of Internet-connected consumer devices may soon be exposed to the same kinds of security threats confronting users of Windows and Mac computers. Air-conditioning units, lighting systems, and TVs that offer networking features typically use bare-bones operating systems that don't include the kinds of exploit defenses Microsoft and Apple have spent years developing.

At the moment, the amount of damage Auriemma can do with his attack is modest when compared with the sophisticated exploits carried out by trojans used to siphon money out of bank accounts. Still, there's nothing stopping him from plundering the contents of USB sticks attached to a vulnerable TV. And with more work, it's possible he could develop firmware that monitors the programs, cameras, or movies it displays.

"A common device like a TV can be used for monitoring people and stealing information," he wrote. "In this situation it doesn't matter if the TV is reachable by the Internet or not because the attacker has a specific selected target: a person at home or a company."

A video demonstration of the hack follows:
ReVuln - The TV is watching you
Update:

In the event a TV is behind a router that uses network address translation, Auriemma's attack won't work at the moment. But with more work, he says it could be possible to use exploits based on IPv6, the next-generation Internet routing protocol, to bypass that protection. He also said readers shouldn't discount the ability to carry out the attack on local networks, since TVs may be plugged into office networks.

Several readers were confused by Auriemma's comment that it doesn't matter if the TV is reachable on the Internet. He said the threat that a TV can be accessed through a network, either by someone cracking a weak Wi-Fi password or someone who has limited network privileges, are two examples of the vulnerability being exploited even if there's no Internet access.

Two days after this article was published Samsung representatives issued the following statement: "We have discovered that only in extremely unusual circumstances a connectivity issue arises between Samsung Smart TVs released in 2011 and other connected devices. We assure our customers that our Smart TVs are safe to use. We will release a previously scheduled software patch in January 2013 to further strengthen Smart TV security. We recommend our customers to use encrypted wireless access points, when using connected

devices."

Sponsor Content

The Right Way to Plan a Migration (Forget Cloud-Washing)

Dan Goodin Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.

Email dan.goodin@arstechnica.com // Twitter @dangoodin001