

أجهزة تلفاز LG الذكية عرضة للاستيلاء الجذري قبل المصادقة عبر الشبكة المحلية



تتيح ثلاث ثغرات في نظام webOS من LG للمهاجمين على نفس الشبكة المحلية الحصول على صلاحيات جذرية على طرازات معينة من أجهزة التلفاز الذكية دون رقم PIN أو تفاعل من المستخدم؛ وقد أصدرت LG تصحيحاً أمنياً.

- يمكن ربط ثلاث ثغرات في نظام webOS من LG لتمكين الوصول الجذري قبل المصادقة من الشبكة المحلية
- لا يتطلب الهجوم إدخال رقم PIN أو أي تفاعل من مالك التلفاز
- تؤثر الثغرة على طرازات محددة من أجهزة تلفاز LG الذكية بما في ذلك 32LQ636BPSA و 27TQ600SW التي تعمل بنظام webOS 7.5.7-25
- أصدرت LG تصحيحاً أمنياً وفقاً لتنبيه SSD Secure Disclosure المنشور في 12 أكتوبر
- يتطلب الاستغلال وجود المهاجم على نفس الشبكة المحلية للجهاز المعرض للخطر

نظرة عامة على الثغرة الأمنية

كشف باحثون أمنيون عن ثلاث ثغرات في نظام التشغيل webOS من LG يمكن استغلالها مجتمعة لمهاجم صلاحيات جذرية كاملة على طرازات معينة من أجهزة التلفاز الذكية. يتطلب مسار الهجوم وجود المهاجم على نفس الشبكة المحلية للجهاز المستهدف، لكنه لا يتطلب أي بيانات اعتماد للمصادقة أو إدخال رقم PIN أو تفاعل من مالك الجهاز.

وفقاً لتنبيه نشرته SSD Secure Disclosure في 12 أكتوبر، تم اختبار سلسلة الثغرات بنجاح على طرازين من أجهزة تلفاز LG: 32LQ636BP و 27TQ600SW، وكلاهما يعمل بنظام webOS الإصدار 7.5.7-25 على البرامج الثابتة الخاصة بهما. اعترفت LG بالمشكلات الأمنية وأصدرت تصحيحاً للأجهزة المتأثرة.

التداعيات على المؤسسات الخاضعة للتنظيم

على الرغم من أن أجهزة التلفاز الذكية الاستهلاكية قد تبدو هامشية بالنسبة للأمن السيبراني المؤسسي الأساسي، إلا أن هذه الأجهزة موجودة بشكل متزايد في البيئات المؤسسية بما في ذلك مكاتب المديرين التنفيذيين وقاعات الاجتماعات والمناطق العامة داخل المؤسسات الخاضعة للتنظيم. يمكن أن يكون جهاز تلفاز ذكي مخترق على شبكة الشركة بمثابة نقطة انطلاق للحركة الجانبية أو استطلاع الشبكة أو تسريب البيانات.

إن طبيعة هذه السلسلة من الثغرات قبل المصادقة مثيرة للقلق بشكل خاص، حيث تتجاوز ضوابط الوصول العادية بالكامل. يمكن للمهاجم الذي يحصل على وصول إلى الشبكة المحلية - سواء من خلال الوجود المادي أو بيانات اعتماد Wi-Fi المخترقة أو ثغرات الشبكة الأخرى - استغلال هذه العيوب دون تشغيل تنبيهات المصادقة أو الحاجة إلى الهندسة الاجتماعية.

التخفيف وإدارة التصحيحات

يجب على المؤسسات إعطاء الأولوية لتحديد جميع أجهزة تلفاز LG الذكية على شبكاتها والتأكد من تطبيق تحديثات البرامج الثابتة على الفور. يقلل توفر تصحيح صادر عن المورد من المخاطر بشكل كبير، ولكن فقط إذا تم نشره بشكل منهجي عبر جميع الأجهزة المتأثرة.

ما يجب فعله الآن

1. إجراء جرد لجميع أجهزة تلفاز LG الذكية المتصلة بشبكات الشركة، بما في ذلك تلك الموجودة في مكاتب المديرين التنفيذيين وقاعات الاجتماعات والمناطق العامة
2. تطبيق تحديث البرامج الثابتة الصادر عن المورد على جميع أجهزة webOS LG المحددة التي تعمل بالإصدار 7.5.7-25 أو الأقدم
3. تنفيذ تجزئة الشبكة لعزل أجهزة التلفاز الذكية وأجهزة إنترنت الأشياء الأخرى عن الأنظمة التجارية الحرجة وشبكات البيانات
4. مراجعة وتقييد ضوابط الوصول إلى الشبكة المحلية، مع ضمان الفصل المناسب بين شبكة Wi-Fi للضيوف والشبكات المؤسسية
5. تحديث قواعد بيانات إدارة الأصول لتشمل جميع الشاشات الذكية وأجهزة إنترنت الأشياء لتتبع الثغرات المستمر

6. إنشاء عملية لإدارة التصديحات للأصول التقنية غير التقليدية بما في ذلك أجهزة التلفاز الذكية والشاشات ومعدات قاعات الاجتماعات