

ثغرة في ISC BIND تتيح هجمات حجب الخدمة عبر استعلامات TKEY



ثغرة في معالجة البيانات بنظام ISC BIND تمكّن المهاجمين عن بُعد من إحداث حالة حجب خدمة من خلال استعلامات TKEY مُصاغة خصيصاً.

- الثغرة CVE-2015-5477 تؤثر على برمجية خادم DNS من نوع ISC BIND بسبب خطأ في معالجة البيانات
- يمكن للمهاجمين عن بُعد استغلال الثغرة عبر استعلامات TKEY لإحداث حجب الخدمة
- يجب على المؤسسات تطبيق التحديثات الأمنية والتدابير الوقائية من المورد فوراً
- على المؤسسات تقييم مدى تعرّض البنية التحتية لنظام DNS للإنترنت
- الالتزام بإرشادات الأمن السيبراني من المورد ضروري للجهات الخاضعة للتنظيم

نظرة عامة على الثغرة

يحتوي برنامج **ISC BIND**، وهو برمجية خادم DNS واسعة الانتشار، على ثغرة في معالجة البيانات مُسجلة برقم **CVE-2015-5477**. تتيح هذه الثغرة للمهاجمين عن بُعد إحداث حالة حجب خدمة من خلال إرسال استعلامات TKEY مُصاغة خصيصاً إلى الخوادم المعرضة للخطر. تشكّل هذه الثغرة مخاطر تشغيلية للمؤسسات التي تعتمد على BIND لخدمات تحليل أسماء النطاقات، وخاصة تلك العاملة في القطاعات الخاضعة للتنظيم حيث تُعد استمرارية الخدمة أمراً بالغ الأهمية.

لا تتطلب الثغرة أي مصادقة ويمكن استغلالها عن بُعد، مما يجعلها هدفاً جذاباً للجهات المهددة التي تسعى لتعطيل البنية التحتية لنظام DNS. يؤدي الاستغلال الناجح إلى انقطاع الخدمة، مما قد يؤثر على استمرارية الأعمال والوصول إلى الأنظمة الحيوية.

المخاطر على المؤسسات السعودية

يجب على المؤسسات الخاضعة للتنظيم في المملكة والتي تشغل خوادم ISC BIND أن تعامل هذه الثغرة كأولوية. تُعد البنية التحتية لنظام DNS أساساً للخدمات الحيوية عبر القطاعات المصرفية والصحية وقطاعات الطاقة والجهات الحكومية. يمكن أن يتسبب هجوم حجب الخدمة ضد خوادم DNS في انقطاعات خدمة أوسع نطاقاً، مما يؤثر على وصول العملاء والعمليات الداخلية وأنظمة الإبلاغ التنظيمي.

يجب على المؤسسات تقييم ما إذا كانت البنية التحتية لنظام DNS معرضة للإنترنت وتقييم الأثر المحتمل لانقطاع الخدمة على التزامات الامتثال والمرونة التشغيلية.

إرشادات المعالجة

تتوفر تحديثات أمنية وتدابير وقائية من المورد لهذه الثغرة. يجب على المؤسسات تطبيق التحديثات وفقاً للنشرات الأمنية الصادرة عن ISC وإجراءات إدارة التغيير الخاصة بها. في حال تعذر التحديث الفوري، يُنصح بتطبيق ضوابط على مستوى الشبكة للحد من معالجة استعلامات TKEY أو تقييد تعرّض خوادم DNS للشبكات غير الموثوقة. يجب على المؤسسات التي تستخدم خدمات DNS السحابية التحقق من أن مزودها قد عالجا هذه الثغرة.

ما يجب فعله الآن

1. تحديد جميع خوادم ISC BIND في بيئتك والتحقق من إصداراتها وحالة التحديثات الأمنية
2. تطبيق التحديثات الأمنية المقدمة من المورد فوراً وفقاً لإجراءات إدارة التغيير
3. تقييم مدى تعرّض البنية التحتية لنظام DNS للإنترنت وتوثيق جميع نُسخ BIND القابلة للوصول خارجياً
4. تطبيق ضوابط شبكية للحد من معالجة استعلامات TKEY أو تقييد تعرّض خوادم DNS في حال تأخر التحديث
5. التحقق من أن مزود خدمات DNS السحابية قد عالجا الثغرة CVE-2015-5477 في بنيتهم التحتية
6. مراجعة إجراءات مراقبة توافر خدمة DNS والاستجابة للحوادث في سيناريوهات حجب الخدمة