تحذير أمني عن ثغرة حديثة في منظومات Oracle

أعلنت شركة Oracle عن اكتشاف ثغرة جديدة في نظام إدارة قواعد البيانات Oracle Database ضمن المكوّن Java VM Component، وقد تم تسجيل هذه الثغرة برمز التعريف CVE-2018-3110، حصلت هذه الثغرة على درجة CVSS Base Score: 9.9 أي أنها ثغرة عالية مستوى الخطورة، وقد أصدرت الشركة بالتزامن مع إعلانها عن الثغرة قائمة تحديثات Patches من أجل إغلاقها، وقد قامت بنشر هذه التحديثات على موقعها الرسمي.

التأثير Impact

قد يتمكن المهاجمون بعد نجاحهم في استغلال هذه الثغرة من السيطرة على المكوّن Java VM، ومنها سيحاول المهاجمون التأثير على العديد من المكونات والتطبيقات الأخرى وذلك بحسب حالة المخدم، مما يسمح لهم بالسيطرة شبه الكاملة على قواعد البيانات Oracle Database بالإضافة إلى تمكنهم من الوصول إلى المخدم الرئيسي الذي يقوم بتشغيل قواعد البيانات بطريقة الرماز Shell Access.

الاستغلال Exploitation

على المهاجمين عن بعد Remotely Attackers أن يمتلكوا سماحيات منخفضة على نظام إدارة قواعد البيانات ومنها سماحية إنشاء جلسة Create Session Privilege أي أن عليهم القيام بعملية مصادقة Authentication وهو شرط لنجاح استغلال هذه الثغرة، على عملية المصادقة هذه أن تتم عن طريق البروتوكول Oracle Net، بالطبع يفترض بالمهاجم عن بعد استخدام أحد أنواع الاتصالات الشبكية المتوفرة مع المخدم المستهدَف.

الإصدارات المتأثرة Affected Products and Versions

Oracle Database Server 11.2.0.4
Oracle Database Server 12.1.0.2
Oracle Database Server 12.2.0.1
Oracle Database Server 18

الحلول Solutions

نظراً لخطورة هذه الثغرة من حيث التأثير وإمكانية الاستغلال، فإن شركة Oracle توصي وبشدة بتطبيق التحديثات على الإصدارات المتأثرة لإغلاق هذه الثغرة بالسرعة الممكنة وبدون أي تأخير، ويشترط لتطبيق التحديثات أن يكون المخدم متضمناً المنتج Oracle Database Server، تم نشر تفاصيل هذه التحديثات ضمن نشرة Oracle Critical Patch Update Advisory -July 2018 أو اختصاراً July 2018 CPU.

تفاصيل إضافية More Details

http://www.oracle.com/technetwork/security-advisory/alert-cve-2018-3110-5032149.html
http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html