الجمهورية العربية السورية
الهيئة الوطنية لخدمات الشبكة
مركز أمن المعلومات

National Agency for Network Services
Information Security Center

تحذير عن ثغرة جديدة في محمّلات الإقلاع GRUB2
"Hole in the Boot/ BootHole" Vulnerability

تم الكشف مؤخراً عن ثغرة جديدة في محمّلات الإقلاع الشهيرة GRand Unified Boot Loaders المستخدَمة في معظم أنظمة التشغيل Linux بالإضافة إلى تأثيرها على أنظمة التشغيل التي تعتمد تقنية الإقلاع الآمن Secure Boot حتى في حال عدم استخدامها لمحمّلات الإقلاع GRUBs ، وقد تم تسجيل هذه الثغرة برمز التعريف CVE-2020-10713، تُصنف هذه الثغرة في فئة ثغرات تنفيذ الرمازات التعسّفية ضمن محمّلات الإقلاع Bootloader Arbitrary Code Execution.

التأثير Impact

إن الاستغلال الناجح لهذه الثغرة سيسمح للمهاجمين بتجاوز إجراءات الإقلاع الآمن Secure Boot Bypass ومن ثم تنفيذ رمازات تعسفية ضمن سياق البيئة التنفيذية لتقنيات الإقلاع Unified Extensible Firmware Interface UEFI، بحيث سيتمكن هؤلاء من إجراء العديد من العمليات مثل إطلاق برمجيات خبيثة، تغيير وتعديل إجرائية الإقلاع، التأثير المباشر على نواة أنظمة التشغيل بالإضافة إلى عدد من العمليات الخبيثة الأخرى التي سيتم تنفيذها مباشرةً قبل عملية إقلاع هذه الأنظمة.

الاستغلال Exploitation

يعتمد المهاجمون على إطلاق هجمة تجاوز سعة المخزن المؤقت Buffer Overflow وذلك أثناء تنفيذ ملف الإعداد grub.cfg الخاص بمحمّلات الإقلاع GRUBs وسيتم كل ذلك ضمن ذاكرة الجهاز المستهدَف، حيث سيحصل المهاجمون على شكل من أشكال الاستغلال المستمر Persistent Exploitation مباشرةً بعيد بداية الإقلاع، سيتطلب الاستغلال الناجح لهذه الثغرة من المهاجم الحصول المسبق على صلاحيات إدارية Administrator Privileges أو وصول فيزيائي قريب Local Access للجهاز المستهدَف والمتأثّر بالثغرة مما قد يصعّب عملية الاستغلال هذه على المهاجمين إلى حد بعيد.

الأنظمة المتأثّرة Affected Products

تم تحديد المنتجات وأنظمة التشغيل التالية على أنها معرّضة لثغرة BootHole وذلك حتى تاريخ إعداد هذا البحث:

- Microsoft
- Oracle
- Red Hat (Fedora and RHEL)

- Canonical (Ubuntu)
- SuSE (SLES and openSUSE)
- Debian
- Citrix
- VMware

الحلول Solutions

سيتم التعامل مع هذه الثغرة من خلال مجموعة من الاجرائيات المتعددة:

- تعمل الجهات المطوّرة لأنظمة التشغيل المتأثرة على إصدار تحديثات لمحمّلات الإقلاع GRUB2
- تحديث شهادات المصادقة الخاصة بتقنية الإقلاع UEFI وذلك من قبل الجهات المصدّرة لها.
- على المؤسسات والشركات تحديث أنظمة التشغيل المتأثرة لديها إلى الإصدارات الأحدث وذلك من أجل الحصول على هذه التحديثات.

المصادر وتفاصيل إضافية More Details

للاطلاع على تفاصيل إضافية يمكن مراجعة المواقع التالية:

- www.tenable.com
- www.eclypsium.com
- nvd.nist.gov
- portal.msrc.microsoft.com

إعداد

ماجد اسماعيل

دائرة الدراسات والأبحاث

تموز-2020