آسیب پذیری امنیتی 'Venom

این آسیب پذیری به هکر اجازه می دهد تا به طور بالقوه به هر دستگاهی که در شبکه یک مرکز داده قرار دارد نفوذ کند. اگر کد دستکاری شده خاصی به سیستم hypervisor فرستاده شود می تواند کل سیستم را از کار بیاندازد. این مساله می تواند به هکر اجازه دهد تا ماشین مجازی خود را ایجاد کند و به ماشین های دیگر دسترسی یابد.

Jason Geffner، محقق امنیتی که این مشکل را کشف کرده است اظهار داشت: میلیون ها ماشین مجازی در حال استفاده از این پلت فرم های آسیب پذیر می باشند

VENOM مخفف Virtual Environment Neglected Operations Manipulation است که درایور کنترلر فلاپی دیسک برای QEMU را تحت تأثیر قرار داده است.

خبر خوب اینکه :

این مشکل در نمونه ساز یارانه منبع باز QEMU یافت شده است. بسیاری از پلت فرم های مجازی سازی مدرن از جمله Xen، KVM و Oracle's VirtualBox دارای این کد خطا می باشند. پلت فرم های VMware، Microsoft Hyper-V و Bochs hypervisors تحت تاثیر این مشکل قرار ندارند و در شبکه های تحت کنترل ما که همگی از Hyper-v و یا VMware استفاده میکنند مشکلی وجود ندارد

برای سوء استفاده از این آسیب پذیری هکر باید بتواند با حق دسترسی root به یک ماشین مجازی دسترسی یابد و کاری که هکر میتواند انجام دهد به چیدمان شبکه بستگی دارد. در حال حاضر کد سوء استفاده از این آسیب پذیری برای راه اندازی حملات وجود ندارد.اصلاحیه های مربوط به این آسیب پذیری به زودی منتشر خواهند شد.