

Alerta de seguridad cibernética	9VSA20-00243-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de junio de 2020
Última revisión	11 de junio de 2020

## NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afectada a actualizaciones.

## Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información obtenida de Xen referente a vulnerabilidad que afecta al sistema de virtualización de código abierto. El presente informe incluye la respectiva medida de mitigación.

## Vulnerabilidad

CVE-2020-0543

## CVE-2020-0543

Debido a la incompleta limpieza de algunos registros de lectura específicos en ciertos tipos de procesadores, un usuario malicioso en una máquina invitada podría obtener acceso a información sensible de otros procesadores como el "Random Number Generator" (instrucciones RDRAND/RDSEED).

### Productos Afectados

Todos los sistemas con arquitectura x86 de Intel que utilicen Xen son vulnerables.

No se ha comprobado que otras arquitecturas y otros procesadores (como ARM) sean vulnerables.

### Mitigación

No se ha publicado una mitigación oficial para esta vulnerabilidad, pero se ha desarrollado un microcódigo aplicable en todas las versiones posteriores o igual a la 4.13 de Xen, el cual puede ser cargado a través de boot (cargado de SO) o en runtime (durante la ejecución del SO).

Las instrucciones para la aplicación del microcódigo se encuentran disponibles en el enlace oficial de Xen publicado al final del documento.

Se está desarrollando los parches para las versiones restantes afectadas, los cuales podrán estar disponibles a través de una actualización de firmware, o a través de la carga del SO.

### Enlaces

<https://xenbits.xen.org/xsa/advisory-320.html>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0543>