BOLETÍN DE ALERTA

Boletín Nro.: 2021-22

Fecha de publicación: 13/09/2021

Tema: Vulnerabilidades críticas en Citrix Hypervisor.

Productos afectados:

- Citrix Hypervisor 8.2 LTSR, anterior a la revisión CTX324257.
- Citrix Hypervisor 7.1 LTSR CU2, anterior a la revisión CTX324256.

Descripción:

Se han descubierto varios problemas de seguridad en Citrix Hypervisor que, en conjunto, pueden permitir que la ejecución de código privilegiado en una máquina virtual invitada comprometa o bloquee el host.

Estos problemas tienen los siguientes identificadores:

- CVE-2021-28694: (Host DoS) de severidad media con una puntuación 6.8.
  Ejecución de código privilegiado malintencionado en una máquina virtual invitada que se ejecuta en un host con firmware que declara tablas ACPI que incluyen regiones de memoria asignadas por identidad para dispositivos que el administrador del host asignó explícitamente a esa máquina virtual invitada en modo de paso a través de PCI.

- CVE-2021-28697: (Compromiso del Host) de severidad alta con una puntuación 7.8
  Ejecución de código privilegiado malintencionado en una máquina virtual invitada que tiene dos o más CPU virtuales asignadas

- CVE-2021-28698: (Host DoS) de severidad media con una puntuación 5.5.
  Ejecución de código privilegiado malicioso en una máquina virtual invitada

- CVE-2021-28699: (Compromiso del Host) de severidad media con una puntuación 5.5

Ejecución de código privilegiado malicioso en una máquina virtual invitada en un host donde el administrador del host ha modificado los límites de la tabla de concesión de invitados o hosts.

- CVE-2021-28701: (Compromiso del Host)
  Ejecución de código privilegiado malicioso en una máquina virtual invitada que tiene dos o más CPU virtuales asignadas.

Impacto:

La explotación exitosa de las vulnerabilidades puede permitir a un atacante tomar el control total del host.

Solución:

Citrix ha publicado revisiones para solucionar estos problemas. Desde el CERT-PY recomendamos a los usuarios afectados instalar las revisiones según lo permita su programa de actualizaciones. Las revisiones se pueden descargar desde las siguientes ubicaciones:

- Citrix Hypervisor 8.2 LTSR: CTX324257 - https://support.citrix.com/article/CTX324257
- Citrix Hypervisor 7.1 LTSR CU2: CTX324256 - https://support.citrix.com/article/CTX324256

Información adicional:

- https://support.citrix.com/article/CTX325319