Alerta de seguridad informática	9VSA20-00159-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de marzo de 2020
Última revisión	18 de marzo 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 afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de VMware referente a dos vulnerabilidades que afectan a los productos VMware Fusion, VMware Workstation, VMRC y VMware Horizon Client, las cuales de ser explotadas permitirían a un atacante local realizar ataques de denegación de servicios y ejecutar código arbitrario en el sistema. Este informe incluye la respectiva mitigación.

Vulnerabilidades

CVE-2020-3950
CVE-2020-3951

Impactos

CVE-2020-3950
Debido al incorrecto uso de los binarios 'setuid', un usuario local podría explotar esta vulnerabilidad para ejecutar código arbitrario en el sistema afectado con privilegios elevados.

CVE-2020-3951
Debido a un error en memoria dentro de 'Cortado Thinprint', un usuario local podría causar un desbordamiento del montón en memoria, botando el servicio Thinprint y causando una denegación de servicios.

Productos Afectados

VMware Workstation Pro / Player
VMware Fusion Pro / Fusion
VMware Remote Console para Mac
VMware Horizon Client para Mac y Windows

Mitigación

Aplicar las actualizaciones publicadas por VMware.

Enlaces

https://www.vmware.com/security/advisories/VMSA-2020-0005.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3950
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3951

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.03.18 22:01:15 -03'00'