| | |
|---|---|
| Alerta de seguridad cibernética | 9VSA20-00304-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 15 de octubre de 2020 |
| Última revisión | 15 de octubre 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 la información obtenida de VMware respecto a vulnerabilidad que afecta al método de autenticación de Horizon DaaS. El presente informe incluye la respectiva medida de mitigación.

## Vulnerabilidad

CVE-2020-3977

Debido a un error en la forma que se maneja el primero factor de autenticación, un atacante con una cuenta válida en Horizon DaaS podría evadir el proceso de autenticación de dos factores para obtener acceso a una cuenta.

## Productos Afectados

Horizon DaaS versiones 8.x y 7.x para cualquier SO.

## Mitigación

En caso de estar utilizando una versión vulnerable, se debe actualizar a la versión 8.0.1 para mitigar esta vulnerabilidad.

## Enlaces

https://www.vmware.com/security/advisories/VMSA-2020-0021.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3977