| | |
|---|---|
| Alerta de seguridad cibernética | 9VSA20-00224-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 26 de mayo de 2020 |
| Última revisión | 26 de mayo 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 OpenConnect referente a vulnerabilidad que afecta a su servicio VPN. El presente informe incluye la respectiva medida de mitigación.

## Vulnerabilidad

CVE-2020-12823

# CVE-2020-12823

Debido a un error en memoria con la función “get_cert_name()” en “gnutls.c”, es posible para un atacante enviar datos de certificado especialmente diseñado para causar una denegación de servicios a una víctima conectada a su servicio, o hasta la ejecución de código arbitrario en el sistema de la víctima.

## Productos Afectados

OpenConnect VPN desde la versión 3.99 hasta la 8.09.

## Mitigación

Aplicar parche entregado por desarrolladores.

## Enlaces

https://gitlab.com/openconnect/openconnect/-/merge_requests/108
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12823