Alerta de seguridad cibernética	9VSA20-00317-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de noviembre de 2020
Última revisión	05 de noviembre 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 Mozilla referente a una vulnerabilidad que permite acceder a la cuenta de usuario en Mozilla VPN. El presente informe incluye las respectivas medidas de mitigación.

Vulnerabilidad

CVE-2020-15679

Vulnerabilidad de fijación de sesión OAuth que permite a un atacante utilizar un enlace de conexión especialmente diseñado, para que un usuario de Mozilla VPN acceda a este, ingrese sus credenciales, y estas puedan ser robadas. Este ataque solo podía ser realizado si el atacante y víctima comparten la misma IP de origen y permite ver los estados de sesión y desconectarlas.

Productos Afectados

Mozilla VPN para Android versión 1.1.0.
Mozilla VPN para Windows versiones anteriores a la 1.2.2.
Mozilla VPN para iOS versión 1.0.7

Mitigación

Actualizar a la versión 1.1.0 (1360) de Mozilla VPN para Android.
Actualizar a la versión 1.0.7 (929) de Mozilla VPN para iOS.
Actualizar a la versión 1.2.2 de Mozilla VPN para Windows.

Enlaces

https://www.mozilla.org/en-US/security/advisories/mfsa2020-48/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15679