

Alerta de seguridad informática	9VSA-00089-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de noviembre de 2019
Última revisión	22 de noviembre de 2019

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 afectada a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida del sitio oficial de Microsoft, referente a una vulnerabilidad que afecta a su aplicación móvil de mensajería, Outlook, la cual, si es explotada, puede resultar en un ataque de tipo spoofing (suplantación de usuario). Este informe incluye la respectiva actualización para mitigar el riesgo.

Vulnerabilidad

- CVE-2019-1460

Impacto

Un atacante podría enviar un correo especialmente diseñado a la víctima, con el cual es posible ejecutar ataques Cross-site Scripting en el sistema afectado, suplantando la cuenta de la víctima.

Producto Afectado

Todas las versiones de Microsoft Outlook para Android, desde la 1.2.33 hasta la 4.0.60 (incluidas).

Mitigación

Actualizar la aplicación a su última versión, 4.0.65, a través de la Play Store.

Enlaces

- <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1460>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1460>