

| | |
|---------------------------------|------------------------------|
| Alerta de seguridad cibernética | 9VSA22-00709-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Crítico |
| TLP | Blanco |
| Fecha de lanzamiento original | 27 de septiembre de 2022 |
| Última revisión | 27 de septiembre de 2022 |

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 CSIRT de Gobierno. La información contenida en los informes o comunicados está afectada a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT de Gobierno, comparte información sobre dos vulnerabilidades que afectan a WhatsApp.

Vulnerabilidades

CVE-2022-36934
CVE-2022-27492

Impacto

Vulnerabilidades de riesgo crítico

CVE-2022-36934: Vulnerabilidad provocada por un error de desborde de enteros. Un atacante puede realizar inyección remota de código a través de una videollamada.

CVE-2022-27492: Un atacante puede realizar inyección remota de código con el envío de un video especialmente diseñado.

Productos afectados

CVE-2022-36934:
WhatsApp for Android anterior a 2.22.16.12
WhatsApp Business for Android anterior a 2.22.16.12
WhatsApp for iOS anterior a 2.22.16.12
WhatsApp Business for iOS anterior a 2.22.16.12

CVE-2022-27492:
WhatsApp for Android anterior a v2.22.16.2, WhatsApp for iOS v2.22.15.9

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor cuando estas estén disponibles.

Enlaces

<https://www.whatsapp.com/security/advisories/2022/?lang=en>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-36934>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27492>