

Alerta de seguridad informática	9VSA-00048-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de septiembre de 2019
Última revisión	11 de septiembre 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 afecta a actualizaciones.

## Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Microsoft en su reporte mensual de actualizaciones correspondiente a septiembre del 2019, parchando un total de 79 vulnerabilidades en sus softwares. Del total anterior, 17 han sido clasificados como críticos, 61 como importantes y uno como moderado.

Además se recalca que 4 de los parches críticos hacen referencia a vulnerabilidades de ejecución remota arbitraria de código o RCE (por sus siglas en inglés) para la aplicación integrada de cliente de escritorio remoto de Windows, lo que podría permitir que un servidor RDP malicioso comprometa el equipo del cliente.

A diferencia del error de BlueKeep, las vulnerabilidades RDP recién parcheadas son todas del lado del cliente, lo que requiere que un atacante engañe a las víctimas para que se conecten a un servidor RDP malicioso a través de ingeniería social, envenenamiento de DNS o utilizando una técnica Man in the Middle (MITM).

## Vulnerabilidad

### Informados en el boletín de septiembre

CVE-2019-1142	CVE-2019-1247	CVE-2019-1263
CVE-2019-1209	CVE-2019-1248	CVE-2019-1264
CVE-2019-1216	CVE-2019-1249	CVE-2019-1265
CVE-2019-1219	CVE-2019-1250	CVE-2019-1274
CVE-2019-1231	CVE-2019-1251	CVE-2019-1282
CVE-2019-1240	CVE-2019-1252	CVE-2019-1283
CVE-2019-1241	CVE-2019-1254	CVE-2019-1286
CVE-2019-1242	CVE-2019-1257	CVE-2019-1293
CVE-2019-1243	CVE-2019-1259	CVE-2019-1295
CVE-2019-1244	CVE-2019-1260	CVE-2019-1296
CVE-2019-1245	CVE-2019-1261	CVE-2019-1297
CVE-2019-1246	CVE-2019-1262	CVE-2019-1299

### Informados adicionalmente

CVE-2019-0928	CVE-2019-1253	CVE-2019-1284
CVE-2019-1138	CVE-2019-1256	CVE-2019-1285
CVE-2019-1208	CVE-2019-1266	CVE-2019-1287
CVE-2019-1214	CVE-2019-1267	CVE-2019-1289
CVE-2019-1215	CVE-2019-1268	CVE-2019-1292
CVE-2019-1217	CVE-2019-1269	CVE-2019-1294
CVE-2019-1220	CVE-2019-1270	CVE-2019-1298
CVE-2019-1221	CVE-2019-1271	CVE-2019-1300
CVE-2019-1232	CVE-2019-1272	CVE-2019-1301
CVE-2019-1233	CVE-2019-1273	CVE-2019-1302
CVE-2019-1235	CVE-2019-1277	CVE-2019-1303
CVE-2019-1236	CVE-2019-1278	CVE-2019-1305
CVE-2019-1237	CVE-2019-1280	CVE-2019-1306

### CVE asociados a vulnerabilidades de cliente RDP

CVE-2019-0787  
CVE-2019-0788  
CVE-2019-1290  
CVE-2019-1291

## Productos Afectados

- Microsoft Windows
- Internet Explorer
- Microsoft Edge (EdgeHTML-based)
- ChakraCore
- Microsoft Office and Microsoft Office Services and Web Apps
- Adobe Flash Player
- Microsoft Lync
- Visual Studio
- Microsoft Exchange Server
- .NET Framework
- Microsoft Yammer
- .NET Core
- ASP.NET
- Team Foundation Server
- Project Rome
- Cliente RDP

## Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

## Enlace

<https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/24f46f0a-489c-e911-a994-000d3a33c573>

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0787>

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0788>

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0928>

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1138>

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1142>

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1208>

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1209>

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1214>

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1215>

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1216>

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1217>

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1219>

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1220>

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1221>

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1231>

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1232>

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1233>

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1235>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1236>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1237>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1240>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1241>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1242>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1243>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1244>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1245>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1246>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1247>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1248>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1249>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1250>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1251>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1252>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1253>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1254>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1256>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1257>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1259>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1260>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1261>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1262>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1263>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1264>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1265>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1266>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1267>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1268>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1269>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1270>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1271>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1272>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1273>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1274>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1277>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1278>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1280>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1282>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1283>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1284>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1285>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1286>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1287>

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1289>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1290>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1291>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1292>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1293>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1294>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1295>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1296>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1297>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1298>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1299>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1300>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1301>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1302>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1303>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1305>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1306>