Alerta de seguridad cibernética	9VSA20-00241-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de junio de 2020
Última revisión	10 de junio 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 entregada por Microsoft en su reporte mensual de actualizaciones correspondiente a junio de 2020, parchando 36 vulnerabilidades en sus softwares clasificando a 2 de ellas como críticas y 34 como importantes, además se informa de 95 vulnerabilidades adicionales al reporte mensual, 10 de ellas clasificadas como críticas, 84 como importantes y 1 como moderada.

Vulnerabilidades

Informadas en el reporte mensual correspondiente al mes de abril

ADV200010	CVE-2020-1223	CVE-2020-1295
CVE-2020-1181	CVE-2020-1225	CVE-2020-1296
CVE-2020-1148	CVE-2020-1226	CVE-2020-1297
CVE-2020-1160	CVE-2020-1229	CVE-2020-1298
CVE-2020-1163	CVE-2020-1232	CVE-2020-1301
CVE-2020-1170	CVE-2020-1242	CVE-2020-1315
CVE-2020-1177	CVE-2020-1261	CVE-2020-1318
CVE-2020-1178	CVE-2020-1263	CVE-2020-1320
CVE-2020-1183	CVE-2020-1268	CVE-2020-1321
CVE-2020-1206	CVE-2020-1284	CVE-2020-1322
CVE-2020-1217	CVE-2020-1289	CVE-2020-1323
CVE-2020-1220	CVE-2020-1290	CVE-2020-1329

De las anteriores se destaca una vulnerabilidad crítica en el protocolo Microsoft Server Message Block 3.1.1 (SMBv3) debido a la forma que maneja ciertas solicitudes. Un atacante que explotara con éxito la vulnerabilidad podría obtener información para comprometer aún más el sistema del usuario.

Para aprovechar la vulnerabilidad contra un servidor, un atacante no autenticado podría enviar un paquete especialmente diseñado a un servidor SMBv3 de destino. Para aprovechar la vulnerabilidad contra un cliente, un atacante no autenticado necesitaría configurar un servidor SMBv3 malicioso y convencer a un usuario para que se conecte a él.

.

Apodado "SMBleed" (CVE-2020-1206) por la empresa de seguridad cibernética ZecOps, el defecto reside en la función de descompresión de SMB, la misma función que con el error SMBGhost o EternalDarkness (CVE-2020-0796), que salió a la luz hace tres meses, potencialmente abriendo sistemas vulnerables de Windows a ataques de malware que pueden propagarse a través de redes.

La vulnerabilidad recién descubierta afecta las versiones de Windows 10 1903 y 1909, para las cuales Microsoft lanzó hoy parches de seguridad como parte de sus actualizaciones mensuales de Patch Tuesday para junio.

Vulnerabilidades adicionales

CVE-2020-0915	CVE-2020-1237	CVE-2020-1281
CVE-2020-0916	CVE-2020-1238	CVE-2020-1282
CVE-2020-0986	CVE-2020-1239	CVE-2020-1283
CVE-2020-1073	CVE-2020-1241	CVE-2020-1286
CVE-2020-1120	CVE-2020-1244	CVE-2020-1287
CVE-2020-1162	CVE-2020-1246	CVE-2020-1291
CVE-2020-1194	CVE-2020-1247	CVE-2020-1292
CVE-2020-1195	CVE-2020-1248	CVE-2020-1293
CVE-2020-1196	CVE-2020-1251	CVE-2020-1294
CVE-2020-1197	CVE-2020-1253	CVE-2020-1299
CVE-2020-1199	CVE-2020-1254	CVE-2020-1300
CVE-2020-1201	CVE-2020-1255	CVE-2020-1302
CVE-2020-1202	CVE-2020-1257	CVE-2020-1304
CVE-2020-1203	CVE-2020-1258	CVE-2020-1305
CVE-2020-1204	CVE-2020-1259	CVE-2020-1306
CVE-2020-1207	CVE-2020-1260	CVE-2020-1307
CVE-2020-1208	CVE-2020-1262	CVE-2020-1309
CVE-2020-1209	CVE-2020-1264	CVE-2020-1310
CVE-2020-1211	CVE-2020-1265	CVE-2020-1311
CVE-2020-1212	CVE-2020-1266	CVE-2020-1312
CVE-2020-1213	CVE-2020-1269	CVE-2020-1313
CVE-2020-1214	CVE-2020-1270	CVE-2020-1314
CVE-2020-1215	CVE-2020-1271	CVE-2020-1316
CVE-2020-1216	CVE-2020-1272	CVE-2020-1317
CVE-2020-1219	CVE-2020-1273	CVE-2020-1324
CVE-2020-1222	CVE-2020-1274	CVE-2020-1327
CVE-2020-1230	CVE-2020-1275	CVE-2020-1331
CVE-2020-1231	CVE-2020-1276	CVE-2020-1334
CVE-2020-1233	CVE-2020-1277	CVE-2020-1340

CVE-2020-1234	CVE-2020-1278	CVE-2020-1343
CVE-2020-1235	CVE-2020-1279	CVE-2020-1348
CVE-2020-1236	CVE-2020-1280	

Impacto y productos afectados

Impacto

Dependiendo de la vulnerabilidad informada por Microsoft se pueden provocar denegaciones de servicio, elevación de privilegios, acceso a información confidencial, ejecución de código remoto o spoofing. El detalle de cada una de las vulnerabilidades se podrá revisar en los enlaces.

Productos Afectados

- Adobe Flash Player (ADV200010)
- Azure DevOps Server 2019
- ChakraCore
- Internet Explorer 9, 11
- Microsoft 365 Apps for Enterprise (32-bit y 64-bit)
- Microsoft Bing Search for Android
- Microsoft Edge (Chromium-based, EdgeHTML-based)
- Microsoft Excel
  - 2010 Service Pack 2 (32-bit y 64-bit editions)
  - 2013 RT Service Pack 1
  - 2013 Service Pack 1 (32-bit y 64-bit editions)
  - 2016 (32-bit y 64-bit editions)
- Microsoft Forefront Endpoint Protection 2010
- Microsoft Office
  - 2010 Service Pack 2 (32-bit y 64-bit editions)
  - 2013 RT Service Pack 1
  - 2013 Service Pack 1 (32-bit y 64-bit editions)
  - 2016 (32-bit y 64-bit editions)
  - 2016 for Mac
  - 2019 (32-bit y 64-bit editions)
  - 2019 for Mac
- Microsoft Project
  - 2010 Service Pack 2 (32-bit y 64-bit editions)
  - 2013 Service Pack 1 (32-bit y 64-bit editions)
  - 2016 (32-bit y 64-bit editions)
- Microsoft Security Essentials
- Microsoft SharePoint
  - Enterprise Server 2013 Service Pack 1
  - Enterprise Server 2016
  - Foundation 2010 Service Pack 2
  - Foundation 2013 Service Pack 1
  - Server 2010 Service Pack 2

- Server 2019
- Microsoft System Center
  - 2012 Endpoint Protection
  - 2012 R2 Endpoint Protection
  - Endpoint Protection
- Microsoft Visual Studio
  - 2015 Update 3
  - 2017 version 15.9 (incluidos 15.1 - 15.8)
  - 2019 version 16.0
  - 2019 version 16.4 (incluidos 16.0 - 16.3)
  - 2019 version 16.6 (incluidos 16.0 - 16.5)
  - Code Live Share extension
- Microsoft Word
  - 2010 Service Pack 2 (32-bit y 64-bit editions)
  - 2013 RT Service Pack 1
  - 2013 Service Pack 1 (32-bit y 64-bit editions)
  - 2016 (32-bit y 64-bit editions)
  - Word para Android
- NuGetGallery
- System Center 2016 Operations Manager
- Windows 10
  - Version 1607, 1709, 1803, 1809, 1903, 1909, 2004, para 32 y 64 bit
- Windows 7
  - 32-bit Systems Service Pack 1
  - x64-based Systems Service Pack 1
- Windows 8.1
  - 32-bit systems
  - x64-based systems
- Windows Defender
- Windows RT 8.1
- Windows Server 2008
  - 32-bit Systems Service Pack 2
  - 32-bit Systems Service Pack 2 (Server Core installation)
  - Itanium-Based Systems Service Pack 2
  - x64-based Systems Service Pack 2
  - x64-based Systems Service Pack 2 (Server Core installation)
  - R2 for Itanium-Based Systems Service Pack 1
  - R2 for x64-based Systems Service Pack 1
  - R2 for x64-based Systems Service Pack 1 (Server Core installation)
- Windows Server 2012
  - 2012
  - Server Core installation
  - R2 y R2 (Server Core installation)
- Windows Server 2016
  - 2016

- Server Core installation
- Windows Server 2019
  - 2019
  - Server Core installation
- Windows Server
  - version 1803 (Server Core Installation)
  - version 1903 (Server Core installation)
  - version 1909 (Server Core installation)
  - version 2004 (Server Core installation)

Mitigación

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-Jun
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200010
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1148
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1160
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1163
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1170
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1177
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1178
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1181
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1183
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1206
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1217
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1220
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1223
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1225
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1226
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1229
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1232
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1242
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1261
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1263
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1268
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1284
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1289
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1290
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1295
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1296
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1297
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1298

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1301
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1315
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1318
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1320
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1321
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1322
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1323
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1329
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0915
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0916
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0986
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1073
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1120
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1162
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1194
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1195
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1196
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1197
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1199
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1201
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1202
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1203
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1204
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1207
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1208
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1209
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1211
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1212
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1213
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1214
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1215
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1216
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1219
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1222
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1230
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1231
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1233
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1234
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1235
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1236
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1237
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1238
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1239
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1241
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1244

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1246
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1247
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1248
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1251
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1253
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1254
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1255
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1257
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1258
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1259
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1260
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1262
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1264
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1265
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1266
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1269
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1270
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1271
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1272
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1273
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1274
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1275
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1276
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1277
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1278
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1279
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1280
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1281
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1282
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1283
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1286
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1287
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1291
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1292
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1293
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1294
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1299
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1300
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1302
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1304
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1305
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1306
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1307
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1309
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1310

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1311
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1312
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1313
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1314
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1316
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1317
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1324
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1327
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1331
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1334
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1340
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1343
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1348