Alerta de seguridad cibernética	9VSA21-00364-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de enero de 2021
Última revisión	14 de enero de 2021

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 Cisco, sobre 68 vulnerabilidades que afectan a varios de sus productos para empresas.

Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

Vulnerabilidades

CVE-2021-1144	CVE-2021-1179	CVE-2021-1201
CVE-2021-1146	CVE-2021-1180	CVE-2021-1202
CVE-2021-1159	CVE-2021-1181	CVE-2021-1203
CVE-2021-1160	CVE-2021-1182	CVE-2021-1204
CVE-2021-1161	CVE-2021-1183	CVE-2021-1205
CVE-2021-1162	CVE-2021-1184	CVE-2021-1206
CVE-2021-1163	CVE-2021-1185	CVE-2021-1207
CVE-2021-1164	CVE-2021-1186	CVE-2021-1208
CVE-2021-1165	CVE-2021-1187	CVE-2021-1209
CVE-2021-1166	CVE-2021-1188	CVE-2021-1210
CVE-2021-1167	CVE-2021-1189	CVE-2021-1211
CVE-2021-1168	CVE-2021-1190	CVE-2021-1212
CVE-2021-1169	CVE-2021-1191	CVE-2021-1213
CVE-2021-1170	CVE-2021-1192	CVE-2021-1214
CVE-2021-1171	CVE-2021-1193	CVE-2021-1215
CVE-2021-1172	CVE-2021-1194	CVE-2021-1216
CVE-2021-1173	CVE-2021-1195	CVE-2021-1217
CVE-2021-1174	CVE-2021-1196	CVE-2021-1237

CVE-2021-1175	CVE-2021-1197	CVE-2021-1307
CVE-2021-1176	CVE-2021-1198	CVE-2021-1360
CVE-2021-1177	CVE-2021-1199	CVE-2021-1147
CVE-2021-1178	CVE-2021-1200	CVE-2021-1148
CVE-2021-1150	CVE-2021-1149	

Impacto

La vulnerabilidad de mayor riesgo es CVE-2021-1144, que afecta al software Cisco Connected Mobile Experiences (CMX), usado para recopilar datos de los clientes y entregar estadísticas en tiempo real, incluso de la ubicación de las personas, realizando seguimiento dentro de las tiendas.

CVE-2021-1144 ocurre debido al manejo incorrecto de los chequeos de autorización al cambiar una contraseña. Para explotar esta falla, el atacante debe tener una cuenta autenticada en CMX, y no requiere privilegios de administrador.

También de alto riesgo es CVE-2021-1237, vulnerabilidad que afecta al cliente de Cisco AnyConnect Secure Mobility para Windows y que permite a atacantes autenticados y locales realizar un ataque de inyección de biblioteca de enlaces dinámicos (DLL).

El resto de las vulnerabilidades afecta la interfaz web de los routers Cisco Small Business RV110W, RV130, RV130W y RV215W. La mayoría permite a un atacante remoto autenticado ejecutar código arbitrario o causar que un aparato afectado se reinicie inesperadamente, mientras que cinco (CVE-2021-1146, CVE-2021-1147, CVE-2021-1148, CVE-2021-1149 y CVE-2021-1150) posibilitan a un atacante remoto autenticado inyectar comandos arbitrarios que son ejecutados con privilegios de super usuario.

Productos afectados

Cisco AnyConnect Secure Mobility Client for Windows, versiones anteriores a la 4.9.04043.
Cisco Connected Mobile Experiences (CMX), versiones 10.6.0 a la 10.6.2.
Routers Cisco Small Business RV110W, RV130, RV130W y RV215W.

Mitigación

Instalar las actualizaciones desde el sitio del proveedor. Cisco no entregó actualizaciones para corregir las vulnerabilidades de los routers Cisco Small Business RV110W, RV130, RV130W y RV215W, ya que entraron en su proceso de fin de vida, por lo que la empresa llama a sus propietarios a migrar a modelos más nuevos.

Enlaces

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-dll-injec-pQnryXLf

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cmxpe-75Asy9k

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1144

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1146

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1159

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1160

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1161

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1162

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1163

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1164

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1165

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1166

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1167

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1168

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1169

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1170

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1171

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1172

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1173

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1174

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1175

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1176

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1177

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1178

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1179

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1180

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1181

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1182

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1183

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1184

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1185

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1186

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1187

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1188

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1189

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1190

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1191

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1192

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1193

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1194

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1195

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1196

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1197

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1198

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1199

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1200

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1201

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1202

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1203

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1204

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1205

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1206

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1207

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1208

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1209

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1210

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1211

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1212

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1213

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1214

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1215

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1216

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1217

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1237

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1307

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1360

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1147

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1148

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1149

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1150

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.01.14 17:05:09 -03'00'