Alerta de seguridad informática	9VSA20-00158-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de marzo de 2020
Última revisión	18 de marzo 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 información obtenida de Trend Micro referente a múltiples vulnerabilidades que afectan a los productos Apex One, OfficeScan y Worry-Free Business Security, las cuales de ser explotadas permitirían a un atacante comprometer completamente al sistema afectado. CSIRT hace un llamado a aplicar las medidas de seguridad lo antes posible, pues existen exploits de día 0 explotando estas vulnerabilidades. Este informe incluye la respectiva mitigación.

Vulnerabilidades

CVE-2020-8467
CVE-2020-8468
CVE-2020-8470
CVE-2020-8598
CVE-2020-8599
CVE-2020-8600

Impactos

CVE-2020-8467
Debido a una validación incorrecta de datos ingresados en el componente 'herramienta de migración', un atacante remoto y autenticado podría enviar peticiones especialmente diseñadas y ejecutar código arbitrario en el sistema afectado, permitiéndole comprometerlo completamente.
Esta vulnerabilidad está actualmente siendo explotada.

CVE-2020-8468
Debido a un error de escape de validación de contenido, un atacante remoto y autenticado podría ingresar datos especialmente diseñados a la aplicación y manipular ciertos componentes del cliente agente, permitiéndole comprometer completamente al sistema afectado.
Esta vulnerabilidad está actualmente siendo explotada.

CVE-2020-8470
Debido a que la aplicación carga librerías DLL de forma insegura, un atacante remoto podría usar un archivo DLL especialmente diseñado y borrar cualquier archivo en el sistema utilizando privilegios SYSTEM.

CVE-2020-8598
Debido a que la aplicación carga librerías DLL de forma insegura, un atacante remoto podría usar un archivo DLL especialmente diseñado y ejecutar comandos arbitrarios en el sistema utilizando privilegios SYSTEM.

CVE-2020-8599
Los servidores de Apex One y OfficeScan contienen un archivo EXE vulnerable, el cual podría permitir a un atacante remoto, ejecutar datos arbitrarios en rutas arbitrarias en las instalaciones afectadas y evadir la autenticación ROOT, comprometiendo completamente al sistema afectado.
No se requiere autenticación para explotar esta vulnerabilidad.

CVE-2020-8600
Debido a un error de validación de entrada al procesar secuencias de directorio trasversal en el parámetro "TempFileName", entregado al endpoint "cgiRecvFile.exe", un atacante remoto podría enviar peticiones HTTP especialmente diseñadas y leer archivos arbitrarios en el sistema, permitiéndole manipular un archivo de llave para evadir autenticación.

Productos Afectados

OfficeScan XG y XG SP1
Apex One 2019
Worry-Free Business Security 9.5 y 10.0

Mitigación

Aplicar las actualizaciones publicadas por Trend Micro.

Enlaces

https://success.trendmicro.com/solution/000245571
https://success.trendmicro.com/solution/000245572
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8467
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8468
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8470
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8598
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8599
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8600

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.03.18 13:44:27 -03'00'