Alerta de seguridad cibernética	9VSA20-00236-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de junio de 2020
Última revisión	06 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 obtenida de FortiNet referente a cinco vulnerabilidades que afectan a sus productos. El presente informe incluye las respectivas medidas de mitigación.

Vulnerabilidades

FG-IR-19-306
CVE-2018-13367
CVE-2019-16150
CVE-2020-9292
CVE-2020-6640

FG-IR-19-306

Debido a la inapropiada neutralización de datos ingresados por el usuario en la página de conexión, un atacante remoto no autenticado podría realizar un ataque XSS reflejado (Reflected Cross-site Scripting) a través de una petición especialmente diseñada, permitiéndole la ejecución de código no autorizado en el servicio afectado.
Impacto: medio.

Productos Afectados
FortiGateCloud versión 4.4.

Mitigación
Actualizar a la versión 20.1 de FortiGateCloud.
Desde el año 2020, FortiGateCloud utilizará una sintaxis nueva para las siguientes versiones.

Enlaces
https://fortiguard.com/psirt/FG-IR-19-306

CVE-2018-13367

Una vulnerabilidad de exposición de información podría permitir a un atacante obtener datos de la plataforma como la versión, a través de un archivo JavaScript, en la interfaz web de usuario FortiOS.
Impacto: bajo.

Productos Afectados
FortiOS versiones 6.2.3, 6.2.0 y anteriores.

Mitigación
Actualizar a la versión 6.2.1, 6.2.2, 6.2.4 o superior de FortiOS.

Enlaces
https://fortiguard.com/psirt/FG-IR-18-173
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13367

CVE-2019-16150

El uso de una llave criptográfica embebida utilizada para encriptar datos de seguridad sensibles en las configuraciones de la aplicación podría permitir a un atacante con acceso a las configuraciones o archivos de respaldo, desencriptar datos sensibles de seguridad.
Impacto: medio bajo.

Productos Afectados
FortiClient para Windows versiones anteriores a la 6.4.0.

Mitigación
Actualizar a la versión 6.4.0 de FortiClient para Windows.

Enlaces
https://fortiguard.com/psirt/FG-IR-19-194
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16150

CVE-2020-9292

Una vulnerabilidad de ruta de servicio sin comillas en el componente "FortiSIEM Windows Agent" podría permitir a un atacante obtener privilegios elevados a traves de la ruta de servicio ejecutable "AoWinAgt".
Impacto: medio.

Productos Afectados
FortiSIEMWindowsAgent versión 3.1.2 y anteriores.

Mitigación
Actualizar a la versión 3.2.0 o superior de FortiSIEMWindowsAgent.

Enlaces
https://fortiguard.com/psirt/FG-IR-20-021
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9292

CVE-2020-6640

Debido a la inapropiada neutralización de datos ingresados por el usuario en el parámetro "Description Area" del perfil administrador, un atacante remoto no autenticado podría enviar un archivo especialmente diseñado a FortiAnalyzer para explotar la vulnerabilidad y realizar un ataque XSS almacenado (Stored Cross-site Scripting), permitiéndole la ejecución de código no autorizado en el servicio afectado.
Impacto: medio.

Productos Afectados

FortiAnalyzer versión 6.2.3 y anteriores.

Mitigación

Actualizar a la versión 6.2.4 o superior, o a la versión 6.4.0 o superior de FortiAnalyzer.

Enlaces

https://fortiguard.com/psirt/FG-IR-20-003
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6640