Alerta de seguridad cibernética	9VSA20-00188-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de abril de 2020
Última revisión	24 de abril 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 F5 referente a múltiples vulnerabilidades que afectan a NGINX Controller. El presente informe incluye la respectiva medida de mitigación.

VULNERABILIDADES

CVE-2020-5863
CVE-2020-5864
CVE-2020-5865
CVE-2020-5866
CVE-2020-5867

CVE-2020-5863

Debido a que el controlador permite a un usuario remoto sin autenticarse agregar usuarios y subir licencias nuevas al sistema, un atacante podría utilizar este comportamiento para consumir todo el espacio en el disco y generar una denegación de servicios en el sistema.

Productos Afectados
NGINX Controller versiones 3.x, 2.x y 1.x.

Mitigación
Actualizar a la versión 3.2.0.

Enlaces
https://support.f5.com/csp/article/K14631834
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8563

CVE-2020-5864

Debido a que la comunicación entre las instancias NGINX Controller y NGINX Plus se saltan la verificación TLS por defecto, un atacante podría utilizar esta condición para realizar un ataque MitM (Man in the Middle) y leer/modificar datos en tránsito.

Productos Afectados
NGINX Controller versiones 3.x, 2.x y 1.x.

Mitigación
Actualizar a la versión 3.2.0.

Enlaces
https://support.f5.com/csp/article/K27205552
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5864

CVE-2020-5865

Debido a que el controlador está configurado para comunicarse sobre canales sin encriptación con su base de datos Postgres, un atacante podría utilizar esta condición para realizar un ataque MitM (Man in the Middle) interceptar los datos en tránsito y leerlos, modificarlos o hasta enviar consultas SQL a la base de datos.

Productos Afectados
NGINX Controller versiones 3.x, 2.x y 1.x.

Mitigación
Actualizar a la versión 3.2.0.

Enlaces
https://support.f5.com/csp/article/K21009022
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5865

CVE-2020-5866

Debido a que el script “helper.sh” usa objetos sensibles como argumentos de consola de comandos, un usuario local podría ganar acceso no autorizado a estos objetos sensibles.

Productos Afectados
NGINX Controller versiones 3.x, 2.x y 1.x.

Mitigación
Actualizar a la versión 3.2.0.

Enlaces
https://support.f5.com/csp/article/K11922628
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5866

CVE-2020-5867

Debido a que el script Agent installer “install.sh” utiliza HTTP en vez de HTTPS para revisar e instalar paquetes, un atacante podría utilizar esta condición para realizar un ataque MitM (Man in the Middle) interceptar los datos en tránsito, y modificarlos para que se descarguen paquetes maliciosos.

Productos Afectados
NGINX Controller versiones 3.x, 2.x y 1.x.

Mitigación
Actualizar a la versión 3.2.0.

Enlaces
https://support.f5.com/csp/article/K00958787
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5867