Alerta de seguridad informática	9VSA20-00208-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de mayo de 2020
Última revisión	09 de mayo 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 NGINX referente a dos vulnerabilidades que afectan a NGINX Controller. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidades

CVE-2020-5894
CVE-2020-5895

CVE-2020-5894

Debido a que el servidor web no invalida correctamente los tokens de sesión del lado del cliente cuando éste se desconecta, un atacante remoto no autenticado podría acceder a este token o hasta adivinarlo, obteniendo acceso no autorizado a la sesión de otro usuario.

CVE-2020-5895

Debido a un error en memoria al procesas mensajes en “Analytics”, “Visibility” y “Reporting daemon”, un atacante remoto podría entregarle mensajes especialmente diseñados a la aplicación, gatillar el error de límites de la memoria y lograr la ejecución de código remoto, comprometiendo completamente al sistema afectado.

Mitigación

Productos Afectados

NGINX Controller versiones 3.x.

Mitigación

Actualizar a la versión 3.4.0 de NGINX Controller.

Enlaces

https://docs.nginx.com/nginx-controller/releases/#nginx-controller-version-3-4-0
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5894
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5895

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.05.09 21:56:43 -04'00'