Alerta de seguridad cibernética	9VSA23-00854-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	27 de junio de 2023
Última revisión	27 de junio de 2023

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 CSIRT de Gobierno. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El CSIRT de Gobierno comparte información de una nuevas vulnerabilidades parchadas por Fortinet en su programa de control de acceso de red FortiNAC, incluyendo una crítica.

Vulnerabilidades

CVE-2023-33299

CVE-2023-33300

Impacto

Vulnerabilidades de riesgo crítico

CVE-2023-33299: Deserialización de datos no confiables, vulnerabilidad que podría permitir a un usuario no autentocado ejecutar código no autorizado o comandos, a través de solicitudes especialmente diseñadas al servicio tcp/1050. CVSS: 9.6.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

FortiNAC versiones 9.4.0 a9.4.2
FortiNAC versiones 9.2.0 a9.2.7
FortiNAC versiones 9.1.0 a9.1.9
FortiNAC versiones 7.2.0 a7.2.1
FortiNAC 8.8 todas las versiones
FortiNAC 8.7 todas las versiones
FortiNAC 8.6 todas las versiones
FortiNAC 8.5 todas las versiones

FortiNAC 8.3 todas las versiones

Enlaces

https://www.fortiguard.com/psirt-monthly-advisory/june-2023-vulnerability-advisories
https://www.fortiguard.com/psirt/FG-IR-23-074
https://www.fortiguard.com/psirt/FG-IR-23-096
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-33299
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-33300

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.06.27 15:20:53 -04'00'