Alerta de seguridad cibernética	9VSA23-00904-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	21 de septiembre de 2023
Última revisión	21 de septiembre 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 nuevas vulnerabilidades críticas, que afectan a Nagios XI y que fueron parchadas en su versión 5.11.2.

Vulnerabilidades

CVE-2023-40931 CVE-2023-40932 CVE-2023-40933 CVE-2023-40934

Impacto

Vulnerabilidades críticas

CVE-2023-40931, CVE-2023-40933 y CVE-2023-40934: La explotación exitosa de estas vulnerabilidades de inyección SQL podrían permitir a un atacante autenticado ejecutar comandos SQL arbitrarios.

CVE-2023-40932: Esta vulnerabilidad puede ser explotada para inyectar JavaScript arbitrario y leer y modificar datos de páginas.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

Nagios XI 5.11.1 y anteriores

Enlaces

https://www.nagios.com/downloads/nagios-xi/change-log/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40931
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40932
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40933
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40934

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.09.21 12:19:01 -03'00'