Alerta de seguridad cibernética	9VSA22-00662-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	20 de junio de 2022
Última revisión	20 de junio de 2022

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 Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT de Gobierno, comparte información sobre nuevas vulnerabilidades en el Siemens SINEC Network Management System (NMS).

Vulnerabilidades

CVE-2021-33722
CVE-2021-33723
CVE-2021-33724
CVE-2021-33725
CVE-2021-33726
CVE-2021-33727
CVE-2021-33728
CVE-2021-33729
CVE-2021-33730
CVE-2021-33731
CVE-2021-33732
CVE-2021-33733
CVE-2021-33734
CVE-2021-33735
CVE-2021-33736

Impacto

Vulnerabilidades de riesgo crítico:

CVE-2021-33723 y CVE-2021-33722: Su explotación en conjunto puede dar a un actor malicioso permisos elevados en el sistema SINEC y acceso total de sistema a NT AUTHORITY\SYSTEM.

Productos afectados

Siemens SINEC NMS, todas las versiones anteriores a la V1.0 SP2 Update 1.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://cert-portal.siemens.com/productcert/pdf/ssa-163251.pdf
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33722

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33723
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33724
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33725
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33726
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33727
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33728
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33729
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33730
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33731
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33732
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33733
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33734
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33735
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33736

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.06.20 16:14:24 -04'00'