Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA20-00348-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de diciembre de 2020
Última revisión	29 de diciembre 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 Nagios Enterprises sobre una vulnerabilidad que afecta a su producto Nagios Core. Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

Vulnerabilidad

CVE-2020-35269

Impacto

La vulnerabilidad CVE-2020-35269 es considerada de riesgo alto, ya que permite a un atacante remoto el realizar ataques de tipo Cross-site Request Forgery (o Falsificación de Petición en Sitios Cruzados). Estos ataques pueden forzar al usuario a ejecutar acciones que no desea en una aplicación en la que esté autenticado, lo que puede ser muy riesgoso gracias al uso de la ingeniería social.

Productos Afectados

Nagios Core 4.2.4.

Mitigación

Instalar las actualizaciones del sitio del proveedor.

Enlaces

https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2020-35269

https://access.redhat.com/security/cve/cve-2020-35269

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-35269