Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA22-00685-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	8 de agosto de 2022
Última revisión	8 de agosto 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 vulnerabilidades críticas que afectan a un producto de Bosch.

Vulnerabilidades

CVE-2022-36301
CVE-2022-36302

Impacto

Vulnerabilidades de riesgo crítico

CVE-2022-36301: Puede permitir a un atacante remoto no autenticado ganar privilegios de Administrador en el aparato aplicando fuerza bruta a una contraseña débil.

Productos afectados

Bosch BF-OS 3.x
La vulnerabilidad es eliminada en BF-OS versión 3.84.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://psirt.bosch.com/security-advisories/bosch-sa-013924-bt.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-36301
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-36302

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.08.08 11:41:57 -04'00'