Alerta de seguridad cibernética	9VSA22-00739-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de noviembre de 2022
Última revisión	04 de noviembre 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 entregada por Fortinet sobre varias vulnerabilidades que afectan a algunos de sus productos.

Vulnerabilidades

CVE-2022-26122	CVE-2022-33878	CVE-2022-39950	CVE-2022-26119
CVE-2022-38374	CVE-2022-38373	CVE-2022-30307	CVE-2022-42473
CVE-2022-35851	CVE-2022-39949	CVE-2022-38380	CVE-2022-33870
CVE-2022-38381	CVE-2022-39945	CVE-2022-35842	CVE-2022-38372

Impacto

Vulnerabilidades de riesgo alto

CVE-2022-38374: Vulnerabilidad de uso inapropiado de la neutralización de inputs durante la generación de páginas web en FortiADC puede permitir a un atacante no autenticado realizar ataques XSS a través de campos HTTP en los logviews de tráfico y eventos.

CVE-2022-35851: Vulnerabilidad de uso inapropiado de la neutralización de inputs durante la generación de páginas web en FortiADC management interface puede permitir a un atacante no autenticado realizar ataques XSS configurando una dirección IP especialmente diseñado.

CVE-2022-38373: Vulnerabilidad de uso inapropiado de la neutralización de inputs durante la generación de páginas web en FortiDeceptor management interface puede permitir a un atacante no autenticado realizar ataques XSS enviando solicitudes con un resource ID de carnada especialmente diseñado.

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

https://www.csirt.gob.cl
Teléfonos: 1510 | + (562) 24863850 | Correo: soc-csirt@interior.gob.cl
@csirtgob
https://www.linkedin.com/company/csirt-gob

CVE-2022-39950: Vulnerabilidad de uso inapropiado de la neutralización de inputs durante la generación de páginas web en los templates de reporte de FortiManager y FortiAnalyzer puede permitir a un atacante con bajo nivel de privilegios realizar ataques XSS al publicar un comentario "protegido" CKeditor.

CVE-2022-26119: Una vulnerabilidad de autenticación inapropiada en FortiSIEM puede permitir a un atacante local con acceso CLI realizar operaciones en el servidor Glassfish directamente a través de una hardcorded password.

CVE-2022-33870: Una neutralización inapropiada de elementos especiales usados en FortiTester puede permitir a un atacante autenticado ejecutar comandos no autorizados.

Productos afectados

AV Engine 0.4.23 a 6.33
FortiMail 6.0.0 a 7.0.2
FortiOS 6.0.0 a 7.2.0
FortiADC 5.0.0 a 7.1.0
FortiClientMac 7.0.0 a 7.0.5
FortiDeceptor 4.0.2 a 4.2.0
FortiEDR 4.0.0 a 5.2.0
FortiAnalyzer 6.0.0 a 7.0.4
FortiManager 6.0.0 a 7.0.4
FortiSIEM 5.0.0 a 6.4.1
FortiSOAR 6.4.0 a 7.2.2
FortiTester 2.3.0 a 7.1.0

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://www.fortiguard.com/psirt?date=11-2022
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26122
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38374
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35851
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38381
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-33878
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38373
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-39949
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-39945
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-39950
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30307
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38380
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35842
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26119
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42473
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-33870
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38372

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.11.04 16:53:58 -03'00'