Alerta de seguridad cibernética	9VSA23-00802-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	10 de marzo de 2023
Última revisión	10 de marzo 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 sobre una vulnerabilidad que afecta a varios productos de Fortinet.

Vulnerabilidades

CVE-2023-25610
CVE-2022-45861
CVE-2022-42476
CVE-2022-29056
CVE-2022-41329
CVE-2023-25605
CVE-2023-25611
CVE-2022-39951
CVE-2022-41333
CVE-2023-23776
CVE-2022-22297
CVE-2022-41328
CVE-2022-40676
CVE-2022-39953
CVE-2022-27490

Impacto

Vulnerabilidades de riesgo crítico

CVE-2023-25610: Vulnerabilidad de tipo “buffer underflow” en la interfaz de administración de FortiOS y FortiProxy permite a un atacante remoto no autenticado ejecutar código arbitrario en el aparato o realizar denegación de servicio en el GUI, a través de solicitudes especialmente diseñadas.

Incluso si corren una versión de FortiOS vulnerable, el hardware listado a continuación no es afectado por la parte de ejecución remota de código de esta vulnerabilidad:

FortiGateRugged-100C
FortiGate-100D
FortiGate-200C
FortiGate-200D
FortiGate-300C
FortiGate-3600A
FortiGate-5001FA2
FortiGate-5002FB2
FortiGate-60D
FortiGate-620B
FortiGate-621B
FortiGate-60D-POE
FortiWiFi-60D
FortiWiFi-60D-POE
FortiGate-300C-Gen2
FortiGate-300C-DC-Gen2
FortiGate-300C-LENC-Gen2
FortiWiFi-60D-3G4G-VZW
FortiGate-60DH
FortiWiFi-60DH
FortiGateRugged-60D
FortiGate-VM01-Hyper-V
FortiGate-VM01-KVM
FortiWiFi-60D-I
FortiGate-60D-Gen2
FortiWiFi-60D-J
FortiGate-60D-3G4G-VZW
FortiWifi-60D-Gen2
FortiWifi-60D-Gen2-J
FortiWiFi-60D-T
FortiGateRugged-90D
FortiWifi-60D-Gen2-U
FortiGate-50E
FortiWiFi-50E
FortiGate-51E
FortiWiFi-51E

FortiWiFi-50E-2R
FortiGate-52E
FortiGate-40F
FortiWiFi-40F
FortiGate-40F-3G4G
FortiWiFi-40F-3G4G
FortiGate-40F-3G4G-NA
FortiGate-40F-3G4G-EA
FortiGate-40F-3G4G-JP
FortiWiFi-40F-3G4G-NA
FortiWiFi-40F-3G4G-EA
FortiWiFi-40F-3G4G-JP
FortiGate-40F-Gen2
FortiWiFi-40F-Gen2

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

Al menos FortiAnalyzer versión 6.0.0 a 6.0.4
Al menos FortiManager versión 6.0.0 a 6.0.4
Al menos FortiPortal 4.1 todas las versiones
FortiPortal 4.2 todas las versiones
FortiAnalyzer 6.4 todas las versiones
FortiAnalyzer versión 6.4.0 a 6.4.10
FortiAnalyzer versión 7.0.0 a 7.0.5
FortiAnalyzer versión 7.2.0 a 7.2.1
FortiAuthenticator versión 5.4 todas las versiones
FortiAuthenticator versión 5.5 todas las versiones
FortiAuthenticator versión 6.0 todas las versiones
FortiAuthenticator versión 6.1 todas las versiones
FortiAuthenticator versión 6.2 todas las versiones
FortiAuthenticator versión 6.3 todas las versiones
FortiAuthenticator versión 6.4 todas las versiones
FortiDeceptor versión 1.0 todas las versiones
FortiDeceptor versión 1.1 todas las versiones
FortiDeceptor versión 2.0 todas las versiones
FortiDeceptor versión 2.1 todas las versiones
FortiDeceptor versión 3.0 todas las versiones
FortiDeceptor versión 3.1 todas las versiones
FortiMail versión 6.0.0 a 6.0.9
FortiMail versión 6.2.1 a 6.2.4
FortiMail versión 6.4.0

FortiNAC todas las versiones 8.8, 8.7, 8.6, 8.5, 8.3
FortiNAC versión 9.1.0 a 9.1.8
FortiNAC versión 9.2.0 a 9.2.6
FortiNAC versión 9.4.0 a 9.4.1
FortiOS 6.0 todas las versiones
FortiOS 6.2 todas las versiones
FortiOS versión 6.4.0 a 6.4.11
FortiOS versión 7.0.0 a 7.0.9
FortiOS versión 7.2.0 a 7.2.3
FortiPortal 5.0 todas las versiones
FortiPortal 5.1 todas las versiones
FortiPortal 5.2 todas las versiones
FortiPortal 5.3 todas las versiones
FortiPortal versión 6.0.0 a 6.0.9 al menos
FortiProxy 1.1 todas las versiones
FortiProxy 1.1 todas las versiones.
FortiProxy 1.2 todas las versiones
FortiProxy 1.2 todas las versiones.
FortiProxy 7.0.x, 2.0.x, 1.2.x, 1.1.x: Impacto es pequeño, ya que no tienen VDOM.
FortiProxy versión 1.1.0 a 1.1.6
FortiProxy versión 1.2.0 a 1.2.13
FortiProxy versión 2.0.0 a 2.0.11
FortiProxy versión 7.0.0 a 7.0.7
FortiProxy versión 7.0.0 a 7.0.8
FortiProxy versión 7.2.0 a 7.2.1
FortiProxy versión 7.2.0 a 7.2.2
FortiRecorder 6.0.11 a 6.0.0
FortiRecorder 6.4.3 y anteriores.
FortiRecorder todas las versiones 2.7
FortiRecorder todas las versiones 6.0
FortiRecorder versión 6.4.0 a 6.4.3
FortiSOAR versión 7.3.0 a 7.3.1
FortiSwitch versión 6.0.0 a 6.0.7
FortiSwitch versión 6.2.0 a 6.2.7
FortiSwitch versión 6.4.0 a 6.4.10
FortiSwitch versión 7.0.0 a 7.0.4
FortiWeb 6.4 todas las versiones
FortiWeb todas las versiones 6.0
FortiWeb todas las versiones 6.1
FortiWeb todas las versiones 6.2
FortiWeb versión 6.3.0 a 6.3.17
FortiWeb versión 6.3.6 a 6.3.20
FortiWeb versión 6.4.0 a 6.4.1
FortiWeb versión 7.0.0 a 7.0.2

Enlaces

https://www.fortiguard.com/psirt-monthly-advisory/march-2023-vulnerability-advisories
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25610
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-45861
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42476
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29056
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41329
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25605
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25611
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-39951
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41333
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23776
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22297
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41328
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-40676
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-39953
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27490

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.03.10 12:55:17 -03'00'