Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

Boletín Informativo

.

05/mayo/2022

Contenido

INTRODUCCIÓN

El siguiente boletín presenta información sobre vulnerabilidades descubiertas por el equipo de F5 que permite a los atacantes realizar un bypass y poder ejecutar comandos dentro del server.

Sugerimos prestar atención a la información mostrada en este documento para poder aplicar las recomendaciones en sus dispositivos.

BIG-IP

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2022_05_05
Clasificación de alerta:	VULNERABILIDAD
Tipo de Impacto:	ALTO
TLP (Clasificación de información):	**WHITE**
Fecha de publicación:	05/05/2022
Es día cero (0 day):	NO

RESUMEN

El proveedor de seguridad y dispositivos de telecomunicaciones, F5, ha publicado una nueva alerta de seguridad para BIG-IP iControl REST. La vulnerabilidad ha sido identificada como CVE-2022-1388 y tiene una puntuación (CVSS v3) de 9.8 de 10.0, categorizada como crítica.

La vulnerabilidad permite a un atacante saltarse la autenticación (bypass) y ejecutar comandos arbitrarios en el servidor, además, la posibilidad de pivotear hacia la red interna.
Debido a la gravedad de la vulnerabilidad y al despliegue generalizado de productos BIG-IP en entornos críticos, el fabricante ha desplegado información sobre la Mitigación inmediata de esta vulnerabilidad.

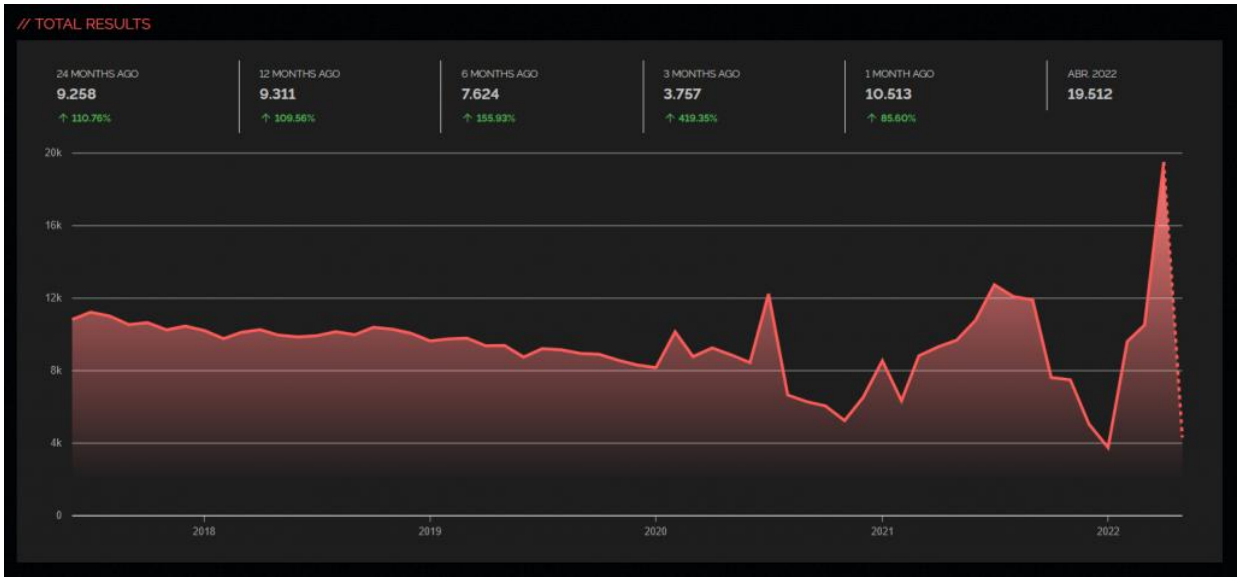
Las versiones afectadas por esta vulnerabilidad son las siguientes:

- BIG-IP versiones 16.1.0 a 16.1.2
- BIG-IP versiones 15.1.0 a 15.1.5
- BIG-IP versiones 14.1.0 a 14.1.4
- BIG-IP versiones 13.1.0 a 13.1.4
- BIG-IP versiones 12.1.0 a 12.1.6
- BIG-IP versiones 11.6.1 a 11.6.5

Tabla de versiones afectadas y parches disponibles:

Producto	Sucursal	Versiones conocidas por ser vulnerables [1]	Correcciones introducidas en	Gravedad	CVSSv3 puntuación [2]	Componente o característica vulnerable
BIG-IP (todos los módulos)	17.x	Ninguna	17.0.0	Crítico	9.8	DESCANSO iControl
	16.x	16.1.0 - 16.1.2	16.1.2.2			
	15.x	15.1.0 - 15.1.5	15.1.5.1			
	14.x	14.1.0 - 14.1.4	14.1.4.6			
	13.x	13.1.0 - 13.1.4	13.1.5			
	12.x	12.1.0 - 12.1.6	No se reparara			
	11.x	11.6.1 - 11.6.5	No se reparara			
Gestión centralizada BIG-IQ	8.x	Ninguna	No aplica	No vulnerable	Ninguna	Ninguna
	7.x	Ninguna	No aplica			
F5OS-A	1.x	Ninguna	No aplica	No vulnerable	Ninguna	Ninguna
F5OS-C	1.x	Ninguna	No aplica	No vulnerable	Ninguna	Ninguna
Trafijo COSUDE	5.x	Ninguna	No aplica	No vulnerable	Ninguna	Ninguna

Segun Shodan, mas de 11,300 dispositivos se encuentran con la interfaz de administración habilitada hacia Internet. En Chile se detectan 212, siendo el país de Latinoamérica con la mayor cantidad de instancias F5 expuestas públicamente.



Mitigación:

Hasta que sea posible instalar una versión fija, puede usar las siguientes secciones como mitigaciones temporales. Estas mitigaciones restringen el acceso a iControl REST solo a redes o dispositivos confiables, lo que limita la superficie de ataque.

- Bloquear el acceso REST de iControl a través de la propia dirección IP
- Bloquear el acceso REST de iControl a través de la interfaz de administración
- Modificar la configuración httpd de BIG-IP:

1. Inicie sesión en TMOS Shell (tmsh) del sistema BIG-IP ingresando el siguiente comando:
`tmsh`

2. Abra la configuración de httpd para editar ingresando el siguiente comando:
`edit /sys httpd all-properties`

3. Busque la línea que comienza con include none y reemplace none con el siguiente texto:
```
"<If \"%{HTTP:connection} =~ /close/i \">
RequestHeader set connection close
</If>
<ElseIf \"%{HTTP:connection} =~ /keep-alive/i \">
RequestHeader set connection keep-alive
</ElseIf>
<Else>
    RequestHeader set connection close
</Else>"
```

4. Presione la tecla ESC, luego use el siguiente comando para guardar (después del comando presionar Y para confirmar los cambios):
`:wq`

5. Guarde la nueva configuración de su BIG-IP con el comando:
`save /sys config`

RECOMENDACIONES

Se recomiendan las siguientes acciones:

- Aplicar las actualizaciones brindadas por el fabricante.
- Si su equipo aun no cuenta con actualizaciones disponibles, puede aplicar las 3 configuraciones recomendadas (Bloquear el acceso REST a través de la propia dirección IP, Bloquear el acceso REST a través de la interfaz de administración y modificar la configuración HTTPD)
- Restringir el acceso público mediante ACL.
- Mantener monitoreo sobre las firmas sospechosas detectadas por su IDS/IPS
- Comunicarse a su SOC y solicitar monitoreo exhaustivo sobre sus dispositivos BIG-IP mientras se planifica la ventana de mantenimiento para aplicar actualizaciones y configuraciones en los equipos.

LINKS DE REFERENCIA

Se adjuntan links de referencia en donde se puede obtener más información de terceros:
https://support.f5.com/csp/article/K23605346

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/main/20220505_01_BIG-IP

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757
El Salvador: +(503) 2249 4252
Honduras: +(504) 2283 5904
República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente