Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

CVE-2023-46747
VULNERABILIDAD EN F5 BIG-IP

27/10/2023

CONTENIDO

INTRODUCCIÓN

F5 ha alertado a los clientes de una vulnerabilidad de seguridad crítica que afecta a BIG-IP y que podría dar lugar a la ejecución remota de código no autenticado.

CVE-2023-46747 VULNERABILIDAD EN F5 BIG-IP

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

ID de alerta:	DSOC-CERT_2023_10_27_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	27/10/2023
Es día cero (0 day):	No

RESUMEN

F5 ha alertado a los clientes de una vulnerabilidad de seguridad crítica que afecta a BIG-IP y que podría dar lugar a la ejecución remota de código no autenticado.

Al problema, que tiene su origen en el componente de utilidad de configuración, se le ha asignado el identificador CVE CVE-2023-46747 y tiene una puntuación CVSS de 9,8 sobre un máximo de 10.

“Esta vulnerabilidad puede permitir que un atacante no autenticado con acceso a la red del sistema BIG-IP a través del puerto de administración y/o las direcciones IP propias ejecute comandos arbitrarios del sistema”, dijo F5 en un aviso publicado el jueves. “No hay exposición al plano de datos; Este es solo un problema del plano de control”.

Se ha descubierto que las siguientes versiones de BIG-IP son vulnerables:

- 17.1.0 (corregido en 17.1.0.3 + hotfix-BIGIP-17.1.0.3.0.75.4-ENG)
- 16.1.0 – 16.1.4 (corregido en 16.1.4.1 + hotfix-BIGIP-16.1.4.1.0.50.5-ENG)
- 15.1.0 – 15.1.10 (corregido en 15.1.10.2 + hotfix-BIGIP-15.1.10.2.0.44.2-ENG)
- 14.1.0 – 14.1.5 (corregido en 14.1.5.6 + hotfix-BIGIP-14.1.5.6.0.10.6-ENG)
- 13.1.0 – 13.1.5 (corregido en 13.1.5.1 + hotfix-BIGIP-13.1.5.1.0.20.2-ENG)

A Michael Weber y Thomas Hendrickson, de Praetorian, se les atribuye el descubrimiento y la notificación de la vulnerabilidad el 4 de octubre de 2023.

La compañía de ciberseguridad, en un informe técnico propio, describió CVE-2023-46747 como un problema de omisión de autenticación que puede llevar a un compromiso total del sistema F5 al ejecutar comandos arbitrarios como root en el sistema de destino, señalando que está "estrechamente relacionado con CVE-2022-26377".

Praetorian también recomienda que los usuarios restrinjan el acceso a la interfaz de usuario de administración de tráfico (TMUI) desde Internet.

"Un error de contrabando de solicitudes aparentemente de bajo impacto puede convertirse en un problema grave cuando dos servicios diferentes descargan las responsabilidades de autenticación entre sí", dijeron los investigadores. "El envío de solicitudes al servicio 'backend' que asume la autenticación manejada por el 'frontend' puede dar lugar a un comportamiento interesante".

Producto	Rama	Versiones Vulnerables	Correcciones introducidas en	Severidad	Puntuación CVSSv32	Componente o característica vulnerable
BIG-IP (todos los módulos)	17.x	17.1.0	17.1.0.3 + Revisión-BIGIP-17.1.0.3.0.75.4-ESP3	Crítico	9.8	Utilidad de configuración
	16.x	16.1.0 - 16.1.4	16.1.4.1 + Revisión-BIGIP-16.1.4.1.0.50.5-ESP3			
	15.x	15.1.0 - 15.1.10	15.1.10.2 + Revisión-BIGIP-15.1.10.2.0.44.2-ESP3			
	14.x	14.1.0 - 14.1.5	14.1.5.6 + Revisión-BIGIP-14.1.5.6.0.10.6-ESP3			
	13.x	13.1.0 - 13.1.5	13.1.5.1 + Revisión-BIGIP-13.1.5.1.0.20.2-ESP3			
Gestión centralizada de BIG-IQ	Todo	Ninguno	No aplicable	No es vulnerable	Ninguno	Ninguno

RECOMENDACIONES

Como mitigación, F5 también ha puesto a disposición de los usuarios de las versiones 14.1.0 y posteriores de BIG-IP un script de shell. "**Este script no debe usarse en ninguna versión de BIG-IP anterior a la 14.1.0 o impedirá que se inicie la utilidad de configuración** ", advirtió la compañía.

A continuación, se muestran otras soluciones temporales disponibles para los usuarios:

- Bloquear el acceso a la utilidad de configuración a través de direcciones IP propias
- Bloquear el acceso a la utilidad de configuración a través de la interfaz de administración

Importante: Se recomienda a los clientes que tengan una licencia de modo compatible con FIPS 140-2 que NO utilicen esta mitigación, ya que provocará un error en la comprobación de integridad de FIPS. Para obtener más información, consulte K11402545: Solución de problemas de errores de autocomprobación de FIPS.

A continuación, damos los pasos para realizar la mitigación del script:

- Copie el siguiente script (o descárguelo) y guárdelo en el sistema BIG-IP afectado.
- Inicie sesión en la línea de comandos del sistema BIG-IP afectado como root.
- Si ha descargado el script, cambie el nombre del script a .sh mediante la siguiente sintaxis de comando

mv <path to script>/mitigation.txt <path to script>/mitigation.sh

- Haga que el script sea ejecutable mediante la utilidad chmod mediante la siguiente sintaxis de comando:

chmod +x <path to script>/mitigation.sh && touch <path to script>/mitigation.sh

- Ejecute el script mediante la siguiente sintaxis de comando:
  ***Importante**: En el caso de VIPRION, los invitados de vCMP en VIPRION y los inquilinos de BIG-IP en VELOS, debe ejecutar este script individualmente en cada blade. Para ello, inicie sesión en la dirección IP de administración asignada a cada blade y ejecútelo. Si no asignó una dirección IP de administración para cada blade, es posible que tenga que conectarse a la consola serie y ejecutarla.*

<path to script>/mitigation.sh.

NOTICIA COMPLETA

https://devel.group/blog/cve-2023-46747-vulnerabilidad-en-f5-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