Alerta de seguridad cibernética	9VSA21-00485-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de agosto de 2021
Última revisión	31 de agosto de 2021

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 equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT de Gobierno, comparte información sobre vulnerabilidades en varios productos de F5, incluyendo algunas de alto riesgo.

Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

Vulnerabilidades

CVE-2021-23025
CVE-2021-23026
CVE-2021-23027
CVE-2021-23028
CVE-2021-23029
CVE-2021-23030
CVE-2021-23031
CVE-2021-23032
CVE-2021-23033
CVE-2021-23034
CVE-2021-23035
CVE-2021-23036
CVE-2021-23037
CVE-2021-23038
CVE-2021-23039
CVE-2021-23040
CVE-2021-23041
CVE-2021-23042
CVE-2021-23043
CVE-2021-23044
CVE-2021-23045
CVE-2021-23046
CVE-2021-23047
CVE-2021-23048
CVE-2021-23049
CVE-2021-23050
CVE-2021-23051
CVE-2021-23052
CVE-2021-23053

Impactos

Nivel de riesgo alto:

CVE-2021-23025: Vulnerabilidad de ejecución de comandos remotos autenticados existe en la herramienta de Configuración de BIG-IP.

CVE-2021-23026: BIG-IP y BIG-IQ son vulnerabiles a ataques CSRF a través del iControl SOAP.

CVE-2021-23027: Una vulnerabilidad XSS basada en DOM existe en una página no revelada de la herramienta de Configuración de BIG-IP, la que permite a un atacante ejecutar JavaScript en el contresto de un usuario que en ese momento ya ha hecho log-in.

CVE-2021-23028: Cuando perfiles de contenido JSON son configurados para URL como parte de la política de seguridad F5 Advanced Web Application Firewall (WAF) / BIG-IP, y aplicados a un servidor virtual, solicitudes no reveladas pueden causar que el proceso bd en BIG-IP ASM se interrumpa.

CVE-2021-23029: Chequeos insuficientes de los permisos pueden permitir a usuarios autenticados con privilegios de visitas realizar ataques tipo SSRF a través del F5 WAF y la herramienta de Configuración BIG-IP ASM.

CVE-2021-23030: Cuando un perfil de WebSocket está configurado en un servidor virtual, solicitudes no reveladas pueden hacer que bd se interrumpa.

CVE-2021-23031: Un usuario autenticado puede realizar escalamiento de privilegios en BIG-IP Advanced WAF y ASM TMUI.

Los usuarios que utilicen Appliance Mode tendrán Scope:Changed, lo que eleva el puntaje CVSSv3 a 9.9.

CVE-2021-23032: Cuando un sistema BIG-IP DNS está configurado con non-default Wide IP y pool settings, respuestas DNS pueden causar que el Traffic Management Microkernel (TMM) se interrumpa.

CVE-2021-23033: Cuando un perfil de WebSocket está configurado en un servidor virtual, solicitudes no reveladas pueden hacer que bd se interrumpa.

CVE-2021-23034: Cuando un perfil DNS usando un DNS cache resolver está configurado en un servidor virtual, solicitudes no reveladas pueden hacer que e proceso Traffic Management Microkernel (TMM) se interrumpa.

CVE-2021-23035: Cuando un perfil HTTP está configurado en un servidor virtual, luego de una secuencia específica de paquetes, respuestas truncadas pueden causar que el TMM se interrumpa.

CVE-2021-23036: Cuando un perfil BIG-IP ASM y DataSafe están configurados en un servidor virtual, solicitudes no reveladas pueden causar que el TMM se interrumpa.

CVE-2021-23037: Una vulnerabilidad de XSS reflejado existe en una página no revelada de la herramoenta de configuración BIG-IP, que permiet e a un atacante ejecutar JavaScript en el contexto del usuario que ha hecho log-in en ese momento.

Productos Afectados

BIG-IP (todos los módulos)
BIG-IP APM
BIG-IQ

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://support.f5.com/csp/article/K50974556
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23025
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23026
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23027
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23028
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23029
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23030
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23031
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23032
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23033
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23034
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23035
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23036
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23037
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23038
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23039
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23040
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23041
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23042
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23043
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23044
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23045
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23046
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23047
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23048
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23049
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23050
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23051
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23052
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23053

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.08.31 10:35:53 -04'00'