Nro. Alerta:	EC-2022-066	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	09-mayo-2022	**Vulnerabilidades presentes en varios productos de F5 Networks**	V 1.2

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de incidente: Sistema y/o Software Crítico
Nivel de riesgo: Alta

II. ALERTA

F5 Networks; dio a conocer una vulnerabilidad calificada como crítica, que afecta a diferentes versiones de software de los productos BIG-IP; la misma que permitiría a un atacante la ejecución arbitraria de comandos, crear o borrar archivos, o deshabilitar servicios.

Figura 1. Ilustración asociada a F5.
Fuente: f5

III. INTRODUCCIÓN

La empresa F5 Networks**;** a través de un boletín de seguridad, publicó una alerta en referencia a una vulnerabilidad calificada como crítica que afecta a diferentes versiones de productos de la familia BIG-IP.

El ID asignado para esta vulnerabilidad es CVE-2022-1388, la misma que surge de un error en la interfaz REST del iControl framework, usado para comunicarse entre aparatos F5 y los usuarios. Esta vulnerabilidad fue calificada como crítica, teniendo una puntuación de 9.6 en CVSS, de momento no existe un exploit disponible y la vulenrabilidad fue reportada por el propio fabricante.

.

Nro. Alerta:	EC-2022-066	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	09-mayo-2022	**Vulnerabilidades presentes en varios productos de F5 Networks**	V 1.2

IV. VECTOR DE ATAQUE: Remoto

La vulnerabilidad puede permitir a un atacante no autenticado con acceso de red a un sistema BIG-IP a través de un puerto de administración o un self-IP address (direcciones IP en un sistema BIG-IP, usadas para asociarse con VLAN), la ejecución arbitraria de comandos, crear o borrar archivos, o deshabilitar servicios.

V. IMPACTO:

A continuación, se mencionan los impactos asociados a la vulnerabilidad en productos BIG-IP.

Ítem	CVE asociado	Afectación	Impacto
1	CVE-2022-1388	Esta vulnerabilidad puede permitir que un atacante no autenticado con acceso de red al sistema BIG-IP a través del puerto de administración y/o direcciones IP propias ejecute comandos arbitrarios del sistema, cree o elimine archivos o deshabilite servicios. A continuación, se listan las versiones de BIG-IP: • 16.1.0 a 16.1.2 • 15.1.0 a 15.1.5 • 14.1.0 a 14.1.4 • 13.1.0 a 13.1.4 Mientras que las versiones: 12.1.0 a 12.1.6 / 11.6.1 a 11.6.5 (no serán parchados)	Confidencialidad: Completo Integridad: Completo Disponibilidad: Completo

Tabla 1. Impacto de vulnerabilidades
Fuente: Support f5. (CISA, 2022)

VI. RECOMENDACIONES:

El EcuCert recomienda a su comunidad objetivo:

- Revisar periódicamente la información emitida por el fabricante en referencia a esta vulnerabilidad; así mismo prestar atención a la disponibilidad de una versión fija lanzada por f5.

Nro. Alerta:	EC-2022-066	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	09-mayo-2022	**Vulnerabilidades presentes en varios productos de F5 Networks**	V 1.2

- Bloquear el acceso REST de iControl ya sea a través de la propia dirección IP y de la interfaz de administración.
- Modificar la configuración httpd de BIG-IP.
- Estas recomendaciones pueden ser implementadas siguiendo las indicaciones emitidas por el fabricante: https://support.f5.com/csp/article/K23605346

VII. Descargo de responsabilidad

- La información en la presente alerta; se proporciona "tal cual" solo con fines informativos. EcuCERT no respalda ningún producto o servicio comercial, incluidos los sujetos de análisis.
- Cualquier referencia a productos, procesos o servicios comerciales específicos por marca de servicio, marca comercial, fabricante o de otro modo, no constituye ni implica respaldo, recomendación o favorecimiento por parte del EcuCERT.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

VIII. REFERENCIAS:

CISA. (06 de 05 de 2022). *CISA*. Obtenido de CISA: https://www.cisa.gov/uscert/ncas/current-activity/2022/05/04/f5-releases-security-advisories-addressing-multiple

CVE. (s.f.). *CVE MITRE*. Obtenido de CVE MITRE: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1388

f5. (05 de 05 de 2022). *Support F5*. Obtenido de Support F5: https://support.f5.com/csp/article/K23605346

VulDB. (06 de 05 de 2022). *VulDB*. Obtenido de VulDB: https://vuldb.com/es/?id.199100