Reporte de Incidentes

Fecha del Reporte: 11/05/2022 12:00 p. m.

Datos de Contacto de la Entidad		
Nombre de la Entidad: Banco de la República		
Dirección: Cra 7 # 14-78		**Sede: Principal**
Sector: Financiero	**Ciudad: Bogotá**	**Departamento: Bogotá D.C.**
Nombre de Quien Reporta: Julio Álvarez Benitez		
Cargo: Director Departamento de Seguridad Informática	**Número Contacto: Fijo: 3431111 Ext** Número de la extensión	**Celular: 3112337123**
Correo Electrónico: jalvarbe@banrep.gov.co		**Skype:** Escriba su usuario de Skype

Incidente	
Fecha y Hora del descubrimiento: 9/05/2022 12:00 p. m.	**Nombre de la Persona que Detectó el Incidente: Fabio Beltrán Vásquez**
Fecha y Hora de Detección: 9/05/2022 12:00 p. m.	**Nombre del administrador del Activo Informático: Subdirección de Telecomunicaciones**

Descripción Detallada:

Atacante explota vulnerabilidad CVE-2022-1388 via Self Ips en F5 Guest 4.
Corre instrucciones tipo: cmd_data=run util bash -c
Lista archivos, exfiltra la configuración de BIGIP
El mismo u otro atacante borra la configuración y deja fuera de producción el guest 4: cmd_data=run util bash -c ""rm -rf /config" interrumpiendo la comunicación de cualquier recurso en Bogotá con Internet.

Método de Detección:

La vulnerabilidad fue detectada desde el 5 de Mayo. Se inició trámite de remediación, pero la instalación del parche se postergó.

El incidente se detectó cuando el atacante borró la configuración de BIGIP e interrumpió el servicio.

La confirmación del ataque y el mecanismo usado para materializarlo fueron encontrados revisando logs de BIGIP en recolector de eventos.

Acciones Realizadas:
*** Restauración Guest4**
*** Migración a versión no vulnerable**
*** Cambio de passwords de Sistema Operativo de los BIGIP**
*** Extracción de logs para investigación**
*** Verificación de remediación**
*** Está en proceso una revisión más profunda de la configuración de BigIP y de los eventos para determinar compromisos adicionales y sensibilidad de la información exfiltrada**

Acciones Pendientes:
Investigación adicional sobre eventos y configuración

Clasificación del Incidente: Seleccione la clase y tipo de incidente.

Malware: Elija un elemento.
Disponibilidad: Sabotaje
Obtención de Información: Identificación de activos y vulnerabilidades (escaneo)
Intrusiones: Elija un elemento.
Compromiso de Información: Modificación y borrado no autorizado de información
Fraude: Elija un elemento.
Contenido Abusivo: Elija un elemento.
Política de Seguridad: Acceso a servicios no autorizados
Otros:
Escriba la clasificación del incidente, si no se encuentra en las listas desplegables

La respuesta al incidente fue efectiva: SI	**Duración del Incidente: Días 0 Horas 2 Minutos**

Se Identifico el Responsable: ○ SI ◉ NO	**Nombre: N/A Es externo. No hay información para atribución**	**Área:** Escriba el nombre del área, al cual pertenece la persona responsable

Hardware y Software Afectado

Servicios Afectados: ☐ Misionales ☐ Estratégicos ☐ Financieros ☐ Tecnológico ☐ Soporte y Mejora

☐ Servidor ☐ PC ☐ Portátil ☐ BD ☐ Portal WEB ☐ Aplicación ☐ Correo ☐ Equipo Activo ☐ Otros

Descripción Detallada del Activo o Servicio Afectado:

F5 BIGIP Vulnerable a

CVE-2022-1388

A través del borrado de la configuración del F5 BIGIP, se afectó el acceso a Internet, impactando los siguientes servicios:

- Navegación
- Publicación de servicios on-prem al público
- Acceso a servicios en nube desde el Banco
- Otros que requieran conexión con internet

Debido al Incidente:	Alguien no autorizado tuvo acceso a la información: ◉ SI ○ NO
	Se ha impedido a algún usuario el acceso a la información: ◉ SI ○ NO
	Se ha borrado, modificado y eliminado alguna información: ◉ SI ○ NO

Impacto del incidente: ☐ Financiero ☐ Reputacional ☐ Operacional ☐ Legal

Causa Raíz:
Explotación de CVE-2022-1388

Realizo Plan de Mejoramiento: ◉ SI ○ NO

Acciones Planificas para Solución Causa Raíz:

- Remediación de vulnerabilidad mediante actualización de plataforma
- Envío de logs F5 a SIEM para identificación de futuros comportamientos sospechosos
- Revisión de acuerdos de mitigación de vulnerabilidades críticas con áreas de TI

Lecciones Aprendidas:

- Se requiere mejorar la oportunidad con la que las vulnerabilidades críticas son remediadas.

Después de realizar la contención y actividades de mitigación el incidente se encuentra: ◉ Abierto ○ Cerrado	**El incidente ya se había presentado:** ○ SI ◉ NO

Otros:

IoC:

149.34.51.113
94.198.42.75
34.242.49.12
105.155.142.2
103.214.146.5
60.49.63.132
191.101.132.1
185.235.42.114
128.199.114.72
151.248.77.11
185.239.226.17
172.105.16.59
94.198.42.75

Comandos ejecutados por atacante:

…

Contáctanos

Si tienes alguna consulta técnica, comunicarse con CSIRT Gobierno a través de los siguientes canales:

Bogotá: 601 344 22 22 Línea Gratuita Nacional: 018000952525 Op. 2

csirtgob@mintic.gov.co