Vulnerabilidad BIG-IP

BCSC-VULNERABILIDAD-BIG-IP

TLP:WHITE

www.basquecybersecurity.eus

Mayo 2022

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

SOBRE EL BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.

El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Respuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

1. RESUMEN EJECUTIVO

El equipo de F5 ha hecho pública una vulnerabilidad de ejecución remota de código en el componente iControl REST en BIG-IP, un servicio de aplicaciones ampliamente utilizado en empresas que, atendiendo a los registros de Shodan, actualmente se encuentra instalado en más de 16.000 dispositivos expuestos públicamente a Internet.

La vulnerabilidad, registrada bajo el identificador CVE-2022-1388, puede permitir que atacantes no autenticados con acceso a la red ejecuten comandos arbitrarios del sistema, eliminen o modifiquen archivos y deshabiliten servicios en BIG-IP. Según lo anterior, la explotación de este fallo puede conducir a un compromiso total del sistema.

Cabe destacar que probablemente los actores de amenazas comiencen a buscar dispositivos vulnerables en breve. Por lo tanto, se recomienda parchear todos los dispositivos afectados lo antes posible o aplicar las mitigaciones indicadas en el apartado Mitigación / Solución.

2. ANÁLISIS TÉCNICO

La vulnerabilidad, descubierta internamente por el equipo de ciberseguridad de F5, 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 indican los aspectos técnicos dados a conocer hasta el momento, puesto que es una vulnerabilidad relativamente reciente, además, desde el fabricante no se han publicado más detalles puesto que la mayoría de equipos aún no están actualizados:

- CVE-2022-1388: esta vulnerabilidad se encuentra en el componente REST de iControl y permite que un actor malicioso envíe solicitudes no reveladas para eludir la autenticación REST de iControl en BIG-IP.

Actualmente no se tiene constancia de la publicación de ningún exploit para aprovechar esta vulnerabilidad. En adición a lo anterior, y siguiendo la misma línea, ninguna prueba de concepto ha sido divulgada, sin embargo, es posible que aparezca algún exploit debido a la repercusión de la vulnerabilidad reportada. Además, se debe tener en cuenta que las vulnerabilidades que afectan a los dispositivos BIG-IP a menudo son explotadas a gran escala, incluso por grupos patrocinados por estados, por lo que es recomendable que se actualice lo antes posible.

La lista completa de los productos afectados se muestra a continuación:

- 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.

3. MITIGACIÓN / SOLUCIÓN

Como es habitual, para prevenir esta y otras vulnerabilidades, desde el BCSC se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible.

A continuación, se muestra, en una tabla, todas las versiones de BIG-IP afectadas, así como las versiones parcheadas correspondientes:

Producto	Versiones Vulnerables	Versiones Parcheadas
BIG-IP (todos los módulos)	16.1.0 - 16.1.2	16.1.2.2
	15.1.0 - 15.1.5	15.1.5.1
	14.1.0 - 14.1.4	14.1.4.6
	13.1.0 - 13.1.4	13.1.5
	12.1.0 - 12.1.6	No existe parche
	11.6.1 - 11.6.5	No existe parche

De manera adicional, F5 ha proporcionado las siguientes tres mitigaciones efectivas que pueden usarse temporalmente si no es posible aplicar las actualizaciones de seguridad de inmediato:

- **Bloquear el acceso a iControl REST a través de la propia dirección IP**, para ello el usuario debe cambiar la configuración de Port Lockdown para cada dirección IP propia en el sistema.

- **Bloquear el acceso a iControl REST a través de la interfaz de administración**, para ello el usuario debe restringir el acceso de administración solo a usuarios y dispositivos confiables a través de una red segura.

- **Modificar la configuración httpd de BIG-IP.**

Para más información se recomienda al usuario consultar los detalles disponibles en la página oficial del fabricante.

4. REFERENCIAS ADICIONALES

- K55879220: Overview of F5 vulnerabilities (May 2022).
- MITRE: CVE-2022-1388.
- iControlREST Home.
- Critical F5 BIG-IP flaw allows device takeover (CVE-2022-1388).
- F5 Releases Security Advisories Addressing Multiple Vulnerabilities.

Reportar incidente

Si has detectado algún incidente de ciberseguridad, avísanos para que tomemos las medidas oportunas para evitar su propagación.

900 104 891

incidencias@bcsc.eus

Catálogo de ciberseguridad

¿Necesitas ayuda con tu ciberseguridad o la de tu empresa?