Basque CyberSecurity Centre

Vulnerabilidades en BIG-IP y BIG-IQ (CVE-2022-41622, CVE-2022-41800)

BCSC-AVISOS

TLP: CLEAR

www.ciberseguridad.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

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 Repuesta 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:

FIRST Improving Security Together
TF-CSIRT Trusted Introducer
CSIRT.es

1. Aviso de seguridad

El proveedor de seguridad F5 ha publicado revisiones para dos vulnerabilidades, CVE-2022-41622 y CVE-2022-41800, que afectan a sus dispositivos de red BIG-IP y BIG-IQ y que podrían resultar en la ejecución remota de código (RCE) y en el bypass de las restricciones del modo Dispositivo respectivamente. Desde la compañía se ha asignado al más grave de los fallos, con el identificador CVE-2022-41622, una puntuación CVSS de 8.8 con una severidad alta. El segundo, con identificador CVE-2022-41800, tiene una puntuación CVSS de 8.7 y también severidad alta.

2. Recursos afectados

- Todos los módulos de BIG IP, versiones 17.0.0, 16.1.0 a 16.1.3, 15.1.0 a 15.1.8, 14.1.0 a 14.1.5, 13.1.0 a 13.1.5
- BIG-IQ Centralized Management, versiones 8.0.0 a 8.2.0, 7.1.0 (solo para la vulnerabilidad con identificador CVE-2022-41622)

3. Análisis técnico

La vulnerabilidad identificada como CVE-2022-41622 se corresponde con un fallo de ejecución remota de código en BIG-IP y BIG-IQ que son vulnerables a los ataques de falsificación de solicitudes entre sitios (CSRF), de forma que un atacante puede engañar a los usuarios que tienen, al menos privilegios de rol de administrador de recursos, y se autentican mediante la autenticación básica en iControl SOAP para realizar acciones críticas. Un atacante puede aprovechar esta vulnerabilidad sólo a través del plano de control, no a través del plano de datos. Si se explota, la vulnerabilidad puede comprometer todo el sistema.

La vulnerabilidad se encuentra en estado reservado a la espera de publicar sus detalles. Los datos que se conocen son:

CVSS Base: 8.8, alta

CWE: 352 Cross-Site Request Forgery (CSRF)

En cuanto a la CVE-2022-41800, es una vulnerabilidad que se produce cuando un usuario autenticado asignado a la función de Administrador puede eludir las restricciones del modo Dispositivo, utilizando un punto final REST de iControl no revelado, de forma que, en el modo Dispositivo, un usuario autenticado con credenciales de usuario válidas asignadas al rol de Administrador puede eludir las restricciones del modo Dispositivo. El modo de dispositivo se aplica mediante una licencia específica o se puede habilitar o deshabilitar para instancias de invitado de multiprocesamiento virtual en clúster (vCMP) individuales. **Una explotación exitosa puede permitir que el atacante cruce un límite de seguridad**

La vulnerabilidad se encuentra en estado reservado a la espera de publicar sus detalles. Los datos que se conocen son:

CVSS Base: 8.7, alta

CWE: 77 Improper Neutralization of Special Elements used in a Command ('Command Injection')

4. Mitigación / Solución

Para la mitigación de estas vulnerabilidades, desde el BCSC se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen las actualizaciones correspondientes.

Para mitigar el fallo CVE-2022-41622 se puede usar un navegador web único y aislado al administrar el sistema BIG-IP o BIG-IQ, teniendo en cuenta que un ataque no se puede prevenir si se ha autenticado en iControl SOAP en el navegador web con autenticación básica. Este mecanismo de autenticación es poco común y es diferente al uso de la página de inicio de sesión para la utilidad de configuración. **Desde F5 se recomienda no autenticarse con la autenticación básica en el navegador web. Si aparece una ventana de autenticación para la autenticación básica en el navegador web, no se deben proporcionar las credenciales.**

Se recomienda seguir las mejores prácticas para asegurar el acceso a la interfaz de administración y las propias direcciones IP de los sistemas BIG-IP y BIG-IQ, lo que ayudará a minimizar la superficie de ataque. La información detallada se encuentra en el aviso de seguridad ofrecido.

Sobre a la vulnerabilidad CVE-2022-41800, desde F5 se establece que hasta que pueda instalar una versión fija, pueden consultarse en el aviso de seguridad una serie de mitigaciones temporales. Estas mitigaciones restringen el acceso a iControl REST solo a redes o dispositivos confiables, lo que limita la superficie de ataque. El atacante debe tener credenciales válidas para una cuenta administrativa con muchos privilegios, por lo tanto, restringir el acceso aún puede dejar el dispositivo expuesto al riesgo de un movimiento interno malicioso o lateral de otro dispositivo comprometido dentro del rango confiable.

5. Referencias Adicionales

- Aviso de seguridad de vulnerabilidad CVE-2022-41622
- Aviso de seguridad de vulenrabilidad CVE-2022-41800
- CVE-2022-41622
- CVE-2022-41800
- iControl SOAP
- iControl REST

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA