CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

Alerta ante vulnerabilidad crítica en F5 BIG-IP y BIG-IQ

Santiago, 20 de marzo de 2021

TLP: BLANCO

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

Detalles de la alerta

Este resumen de ciberataques, vulnerabilidades e incidentes de seguridad cibernética tiene como propósito destacar algunos eventos de días pasados para que puedan ser interpretados y discutidos por las diferentes entidades que tengan acceso a su lectura.

Este informe reúne los antecedentes conocidos hasta el día de su publicación. La información consignada en el presente documento es catalogada como TLP BLANCO.

El miércoles 10 de marzo de 2021, F5 Networks lanzó varias actualizaciones de seguridad (https://support.f5.com/csp/article/K02566623) para sus dispositivos BIG-IP y BIG-IQ, las que fueron compartidas a su vez por el CSIRT de Gobierno (https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00408-01 y https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00405-01).

Cuatro de las vulnerabilidades fueron catalogadas como riesgo critico de las 21 anunciadas por la empresa F5.

Vulnerabilidades Críticas

- CVE-2021-22986
- CVE-2021-22987
- CVE-2021-22991
- CVE-2021-22992

La empresa explicó que las vulnerabilidades afectan a BIG-IP y BIG-IQ, debido a la gravedad de las vulnerabilidades críticas se recomienda actualizar de forma inmediata las versiones a BIG-IP: 16.0.1.1, 15.1.2.1, 14.1.4, 13.1.3.6, 12.1.5.3 y 11.6.5.3 y BIG-IQ 8.0.0, 7.1.0.3 y 7.0.0.2. (CVE-2021-22986)

La explotación exitosa de estas vulnerabilidades podría llevar a que los sistemas se vean comprometidos, provocando la fuga de datos e interrupciones del servicio hasta el compromiso total del sistema.

Si se encuentra utilizando la implementación BIG-IP Virtual Edition en la nube pública (AWS, Azure, GCP o Alibaba), se recomienda que instale las últimas versiones de BIG-IP.

Resumen de Vulnerabilidad Criticas

CVE-2021-22986: Esta vulnerabilidad permite que los atacantes no autentificados pueden ejecutar comandos por iControl REST, a través de la interfaz de administración y direcciones Ip propias del equipo, permitiendo crear o eliminar archivos y deshabilitar servicios. Esta vulnerabilidad se puede explotar a través solo del plano de control.

CVE-2021-22987: Esta vulnerabilidad afecta a la interfaz de usuario de administración de tráfico (TMUI), permite a los atacantes autentificados con acceso de red ejecutar comandos, permitiendo crear o eliminar archivos y deshabilitar servicios. Esta vulnerabilidad se puede explotar a través solo del plano de control.

CVE-2021-22991: Esta vulnerabilidad de desbordamiento de Búfer puede resultar en un ataque DoS, ya que puede manejar incorrectamente la normalización de URI Traffic Management Microkernel de los servidores virtuales. Esta vulnerabilidad se puede explotar a través solo del plano de datos

CVE-2021-22992: Esta vulnerabilidad de desbordamiento de Búfer permite que los atacantes envíen una respuesta HTTP maliciosa a un servidor virtual provocando un ataque DoS, donde el sistema BiG-IP Advanced WAF / ASM experimente una denegación de servicio. Esta vulnerabilidad puede explotarse a través del plano de control.

Tabla Vulnerabilidades F5 Critica

La siguiente tabla proporciona información clave para determinar la versión afectada y la versión que la mitiga en relación a las vulnerabilidades críticas.

CVE	Severity	CVSS score	Affected products	Affected versions	Fixed versions	Appliance mode / Non-Appliance mode[3]	Control plane / Data plane[4]
CVE-2021-22986	Critical	9.8	BIG-IP (All modules)	16.0.0-16.0.1 15.1.0-15.1.2 14.1.0-14.1.3.1 13.1.0-13.1.3.5 12.1.0-12.1.5.2	16.0.1.1 15.1.2.1 14.1.4 13.1.3.6 12.1.5.3[1]	Both	Control plane – iControl REST
			BIG-IQ	7.1.0-7.1.0.2 7.0.0-7.0.0.1 6.0.0-6.1.0	8.0.0 7.1.0.3 7.0.0.2	N/A	Control plane – iControl REST
CVE-2021-22987	Critical	9.9	BIG-IP (All modules)	16.0.0-16.0.1 15.1.0-15.1.2 14.1.0-14.1.3.1 13.1.0-13.1.3.5 12.1.0-12.1.5.2 11.6.1-11.6.5.2	16.0.1.1 15.1.2.1 14.1.4 13.1.3.6 12.1.5.3[1] 11.6.5.3	Appliance mode	Control plane - TMUI
CVE-2021-22991	Critical	9.0	BIG-IP (All Modules)[2]	16.0.0-16.0.1 15.1.0-15.1.2 14.1.0-14.1.3.1 13.1.0-13.1.3.5 12.1.0-12.1.5.2	16.0.1.1 15.1.2.1 14.1.4 13.1.3.6 12.1.5.3[1]	Both	Data plane
CVE-2021-22992	Critical	9.0	BIG-IP Advanced WAF/ASM	16.0.0-16.0.1 15.1.0-15.1.2 14.1.0-14.1.3.1 13.1.0-13.1.3.5 12.1.0-12.1.5.2 11.6.1-11.6.5.2	16.0.1.1 15.1.2.1 14.1.4 13.1.3.6 12.1.5.3[1] 11.6.5.3	Both	Data plane

Mitigación

F5 Networks ha entregado los procedimientos para realizar la mitificación de estas amenazas. En primer lugar, **recomienda actualizar de forma inmediata** si no es posible puede utilizar algunas **mitigaciones temporales** que se enumeran a continuación.

I. Mitigación CVE-2021-22986[1]

Restringir el acceso a iControl REST solo a redes o dispositivos confiables, lo que limita la superficie de ataque.

a) Bloquear el acceso REST de iControl a través de la dirección IP propia

Puede bloquear todo acceso a la interfaz iControl REST de su sistema BIG-IP a través de direcciones IP propias. Para hacerlo, puede cambiar la configuración de Bloqueo de puerto a No permitir ninguno para cada dirección IP propia en el sistema. Si debe abrir algún puerto, debe usar la opción Permitir personalizado, teniendo cuidado de no permitir el acceso a iControl REST. De forma predeterminada, iControl REST escucha en el puerto TCP 443. Alternativamente, puede configurar un puerto personalizado.

Nota: Realizar esta acción evita todo acceso a la utilidad de configuración y al iControl REST utilizando la dirección IP propia. Estos cambios también pueden afectar a otros servicios, incluida la ruptura de configuraciones de alta disponibilidad (HA).

Antes de realizar cambios en la configuración de sus propias direcciones IP, F5 recomienda encarecidamente que consulte los siguientes artículos:

- K17333[2]: Descripción general del comportamiento de bloqueo de puertos (12.x - 16.x)
- K13092[3]: Descripción general de la protección del acceso al sistema BIG-IP
- K31003634[4]: La utilidad de configuración de Single-NIC BIG-IP Virtual Edition ahora tiene como valor predeterminado el puerto TCP 8443
- K51358480[5]: El VE BIG-IP de una sola NIC puede volver por error al puerto httpd de administración predeterminado después de una recarga de la configuración

[1] https://support.f5.com/csp/article/K03009991
[2] https://support.f5.com/csp/article/K17333
[3] https://support.f5.com/csp/article/K17333
[4] https://support.f5.com/csp/article/K31003634
[5] https://support.f5.com/csp/article/K51358480

b) Bloquear el acceso REST de iControl a través de la interfaz de gestión

Para mitigar esta vulnerabilidad para los productos F5 afectados, debe restringir el acceso de administración solo a usuarios y dispositivos confiables a través de una red segura. Para obtener más información sobre cómo proteger el acceso a los sistemas BIG-IP

Recomienda encarecidamente que consulte los siguientes artículos:

- K13092[6]: Descripción general de la protección del acceso al sistema BIG-IP
- K46122561[7]: Restricción del acceso a la interfaz de administración mediante reglas de firewall de red
- K69354049[8]: Restricción del acceso a la interfaz de administración BIG-IP para la utilidad de configuración y los servicios REST de iControl mediante iptables

II. Mitigación CVE-2021-22987[9]

Este ataque es a través de usuarios legítimos y autentificados, no existe una mitigación viable mientras se permita al usuario o al atacante acceder a la utilidad de configuración. La única forma es eliminar el acceso a los usuarios de no confianza. Y limitar la superficie de ataque permitiendo solo redes o dispositivos de confianza.

a) Bloquear el acceso a la utilidad de configuración a través de direcciones IP propias

Puede bloquear todo acceso a la utilidad de configuración de su sistema BIG-IP utilizando direcciones IP propias. Para hacerlo, puede cambiar la configuración de **Bloqueo de puerto** a **No permitir ninguno** para cada dirección IP propia en el sistema. Si debe abrir algún puerto, debe usar la opción **Permitir personalizado**, teniendo cuidado de no permitir el acceso a la utilidad de configuración. De forma predeterminada, la utilidad de configuración escucha en el puerto TCP 443. Como alternativa, puede configurar un puerto personalizado.

Nota: Realizar esta acción evita todo acceso a la utilidad de configuración y al iControl REST utilizando la dirección IP propia. Estos cambios también pueden afectar a otros servicios, incluida la ruptura de configuraciones de alta disponibilidad (HA).

Antes de realizar cambios en la configuración de sus propias direcciones IP, F5 recomienda encarecidamente que consulte los siguientes artículos:

[6] https://support.f5.com/csp/article/K13092
[7] https://support.f5.com/csp/article/K46122561
[8] https://support.f5.com/csp/article/K69354049
[9] https://support.f5.com/csp/article/K18132488

- K17333[10]: Descripción general del comportamiento de bloqueo de puertos (12.x - 16.x)
- K13092[11]: Descripción general de la protección del acceso al sistema BIG-IP
- K31003634[12]: La utilidad de configuración de Single-NIC BIG-IP Virtual Edition ahora tiene como valor predeterminado el puerto TCP 8443
- K51358480[13]: El VE BIG-IP de una sola NIC puede volver por error al puerto httpd de administración predeterminado después de una recarga de la configuración

b) Bloquear el acceso a la utilidad de configuración a través de la interfaz de administración

Debe restringir el acceso de administración solo a los usuarios y dispositivos confiables a los productos F5 a través de una red segura. Para obtener más información sobre cómo proteger el acceso a los sistemas BIG-IP, consulte los siguientes artículos.

- K13092[14]: Descripción general de la protección del acceso al sistema BIG-IP
- K46122561[15]: Restricción del acceso a la interfaz de administración mediante reglas de firewall de red
- K69354049[16]: Restricción del acceso a la interfaz de administración BIG-IP para la utilidad de configuración y los servicios REST de iControl mediante iptables

III. Mitigación CVE-2021-22991[17]

No hay mitigación alternativa por tanto, se debe actualizar la plataforma según el punto indicado arriba “Tabla Vulnerabilidades F5 Critica.

[10] https://support.f5.com/csp/article/K17333
[11] https://support.f5.com/csp/article/K17333
[12] https://support.f5.com/csp/article/K31003634
[13] https://support.f5.com/csp/article/K51358480
[14] https://support.f5.com/csp/article/K13092
[15] https://support.f5.com/csp/article/K46122561
[16] https://support.f5.com/csp/article/K69354049
[17] https://support.f5.com/csp/article/K56715231

IV. Mitigación CVE-2021-22992[18]

a) Mitigar conexiones maliciosas usando una iRule

Puede asociar la siguiente iRule con los servidores virtuales afectados a la vulnerabilidad ya que IRule examina la respuesta del servidor y devuelve un error 502 para respuestas vulnerables.

Realice el siguiente procedimiento:

1. Inicie sesión en la utilidad de configuración
2. Vaya a Tráfico local > iRules > Lista de iRule .
3. Seleccione Crear.
4. Ingrese un nombre para la iRule.
5. Para la definición , agregue el siguiente código de iRule:

```
# Mitigation for K52510511: Advanced WAF/ASM Buffer Overflow vulnerability CVE-2021-22992
when RULE_INIT {
# Set static::debug 1 to enable debug logging.
    set static::debug 0
    set static::max_length 4000
}
when HTTP_REQUEST {
    if {$static::debug}{
        set LogString "Client [IP::client_addr]:[TCP::client_port] ->
[HTTP::host][HTTP::uri]"
}
        set uri [string tolower [HTTP::uri]]
}
when HTTP_RESPONSE {
    set header_names [HTTP::header names]
    set combined_header_name [join $header_names ""]
    set combined_header_name_len [string length $combined_header_name]
    if {$static::debug}{
        log local0. "=================response====================="
        log local0. "$LogString (response)"
        log local0. "combined header names: $combined_header_name"
        foreach aHeader [HTTP::header names] {
        log local0. "$aHeader: [HTTP::header value $aHeader]"
}
        log local0. "the length of the combined response header names:
$combined_header_name_len"
        log local0. "============================================="
}
    if { ( $combined_header_name_len > $static::max_length ) } {
        log local0. "In the response of '$uri', the length of the combined header names
$combined_header_name_len exceeds the maximum value $static::max_length. See K52510511:
Advanced WAF/ASM Buffer Overflow vulnerability CVE-2021-22992"
HTTP::respond 502 content "<HTML><HEAD><TITLE>Bad Gateway</TITLE></HEAD> <BODY><P>The server
response is invalid. Please inform the administrator. Error: K52510511</P></BODY></HTML>"
}
}
```

[18] https://support.f5.com/csp/article/K52510511

1. Seleccione **Terminado**.
2. Asocie la iRule con los servidores virtuales afectados.

b) Modificar la configuración de la página de inicio de sesión

Puede eliminar la configuración de las dos opciones siguientes de la configuración de la página de inicio de sesión:

- Nombre y valor del encabezado de validación esperado
- Nombre y valor del encabezado de validación no esperado

Realice el siguiente procedimiento:

1. Inicie sesión en la utilidad de configuración del sistema BIG-IP Advanced WAF / ASM afectado.
2. Vaya a **Seguridad** > **Seguridad de la aplicación** > **Sesiones e inicios de sesión** > Lista de páginas de inicio de sesión.
3. Seleccione la política de seguridad de la lista Política actual editada.
4. Seleccione el nombre de la URL de **inicio de sesión de la lista de páginas de inicio de sesión**.
5. Elimine toda la configuración de ambas configuraciones.
6. Seleccione **Guardar** para guardar los cambios.
7. Seleccione **Aplicar política** para aplicar los cambios.
8. Seleccione **Aceptar** para confirmar la operación.

Nota: Estas dos configuraciones deben permanecer vacías hasta que el sistema BIG-IP Advanced WAF / ASM afectado se actualice.

c) Harden pool members

Para mitigar esta vulnerabilidad, puede fortalecer su red y servidores web back-end para evitar que los encabezados maliciosos en la respuesta HTTP a la página de inicio de sesión se envíen al sistema BIG-IP Advanced WAF / ASM. Otros ataques contra el servidor, como CRLF Injection o HTTP Response Splitting, también pueden usarse para manipular la respuesta HTTP. El uso del cumplimiento del protocolo HTTP puede proteger contra estos ataques; consulte K10280[19]: Descripción general del cumplimiento del protocolo HTTP de BIG-IP ASM.

[19] https://support.f5.com/csp/article/K10280

d) Eliminar páginas de inicio de sesión

Puede eliminar cualquier página de inicio de sesión configurada para una política de seguridad y evitar el uso de la función de página de inicio de sesión. Hasta que el sistema BIG-IP Advanced WAF / ASM afectado se actualice.

Para eliminar una página de inicio de sesión, realice el siguiente procedimiento:

1. Inicie sesión en la utilidad de configuración del sistema BIG-IP ASM.
2. Vaya a **Seguridad** > **Seguridad de la aplicación** > **Sesiones e inicios de sesión** > **Lista de páginas de inicio de sesión**.
3. Seleccione la política de seguridad de la lista Política actual editada.
4. Seleccione la configuración de la página de inicio de sesión que desea eliminar.
5. Seleccione **Eliminar**.
6. Seleccione **Aceptar** para confirmar la eliminación.
7. Seleccione **Aplicar política** para aplicar los cambios.
8. Seleccione **Aceptar** para confirmar la operación.

Nota: la configuración de la página de inicio de sesión puede ser fundamental para la función de las funciones de prevención de ataques de fuerza bruta, cumplimiento de inicio de sesión y seguimiento de sesiones en una política de seguridad. Revise su política de seguridad para ver si alguna de estas funciones requiere la configuración de la página de inicio de sesión antes de eliminarla.

Enlaces

Se adjuntan enlaces adicionales a los descritos anteriormente en los pies de página.

Consideraciones y orientación cuando sospecha de un compromiso de seguridad en un sistema BIG
https://support.f5.com/csp/article/K11438344

Descripción general de las vulnerabilidades F5 (marzo de 2021)
https://support.f5.com/csp/article/K02566623

Plataformas compatibles con BIG-IP VE
https://clouddocs.f5.com/cloud/public/v1/matrix.html

Guía de actualización y actualización de BIG-IP | Capítulo 1:
https://support.f5.com/csp/article/K84205182

Comprensión del control de versiones del aviso de seguridad
https://support.f5.com/csp/article/K51812227

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.03.20 18:00:39 -03'00'