Alerta de seguridad cibernética	9VSA20-00200-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de mayo de 2020
Última revisión	02 de mayo de 2020

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

RESUMEN

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por F5 referente a vulnerabilidades que afectan a sus productos. El presente informe incluye las respectivas medidas de mitigación.

VULNERABILIDADES

CVE-2020-5880 CVE-2020-5893
CVE-2020-5889 CVE-2020-5890
CVE-2020-5874 CVE-2020-5873
CVE-2020-5875 CVE-2020-5872
CVE-2020-5883 CVE-2020-5878
CVE-2020-5888 CVE-2020-5892
CVE-2020-5876 CVE-2020-5877
CVE-2020-5884 CVE-2020-5891
CVE-2020-5871 CVE-2020-5881
CVE-2020-5887 CVE-2020-5886
CVE-2020-5879 CVE-2020-5885

CVE-2020-5880

Impacto

El proceso **restjavad** puede exponer una forma para que los atacantes carguen archivos arbitrarios en el sistema BIG-IP, evitando el sistema de autorización. Los mensajes de error resultantes también pueden revelar rutas internas del servidor

Un atacante remoto puede llenar el almacenamiento del disco y hacer que el host BIG-IP no funcione.

Productos Afectados

BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM) versiones:

- 15.x anteriores a 15.1.0
- 14.x anteriores a 14.1.2.4

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://support.f5.com/csp/article/K94325657
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5880

CVE-2020-5889

Impacto

En el acceso al portal BIG-IP APM, una solicitud HTTP especialmente diseñada puede conducir a un XSS reflejado después de que el sistema BIG-IP APM reescriba la respuesta HTTP del servidor backend no confiable y la envíe al cliente.

Un atacante puede crear una URL maliciosa y enviarla a una víctima para lanzar un ataque de cross-site scripting (XSS).

Productos Afectados

BIG-IP (APM), versiones:

- 15.1.0, anteriores a 15.1.0.2
- 15.0.0 – 15.0.1, anteriores a 15.0.1.3
- 14.x, anteriores a 14.1.2.4

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://support.f5.com/csp/article/K24415506
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5889

CVE-2020-5874

Impacto

En determinadas circunstancias, un atacante que envía solicitudes específicamente diseñadas a un servidor virtual BIG-IP APM puede causar una interrupción del servicio proporcionado por el Traffic Management Microkernel (TMM).

Un atacante puede realizar un ataque de denegación de servicio (DoS) en un sistema BIG-IP haciendo que se reinicie el proceso TMM.

El plano de datos solo se ve afectado y expuesto cuando el servidor virtual está configurado para usar OpenID connect. El plano de control no se ve afectado por esta vulnerabilidad.

Productos Afectados

BIG-IP APM, versiones:

- 15.0.0, anteriores a 15.1.0
- 15.0.1, anteriores a 15.0.1.3
- 14.1.0 – 14.1.2, anteriores a 14.1.2.4
- 14.0.0 – 14.0.1, anteriores a 14.0.1.1

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://support.f5.com/csp/article/K46901953
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5874

CVE-2020-5875

Impacto

Bajo ciertas condiciones, el Microkernel de gestión de tráfico (TMM) puede generar un archivo central y reiniciarse mientras procesa el tráfico SSL con un proxy HTTP/2 completo.

Si ha habilitado HTTP/2, Message Routing Framework (MRF) y SSL, una secuencia de solicitud determinada puede desencadenar una condición que puede hacer que TMM genere un archivo central y se reinicie. Un atacante puede hacer que un sistema BIG-IP produzca un archivo central, interrumpiendo el flujo de tráfico y provocando una conmutación por error

Productos Afectados

BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM), versiones:

- 15.0.0, anteriores a 15.1.0
- 15.0.1, anteriores a 15.0.1.1
- 14.1.x, anteriores a 14.1.2.4

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://support.f5.com/csp/article/K65372933
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2020-5875

CVE-2020-5883

Impacto

Cuando un servidor virtual está configurado con un proxy explícito HTTP y tiene una iRule HTTP_PROXY_REQUEST adjunta, las solicitudes POST enviadas al servidor virtual provocan una pérdida de memoria xdata. (CVE-2020-5883)

El sistema BIG-IP puede volverse vulnerable a las condiciones que se producen cuando no hay memoria debido a una pérdida de memoria.

Productos Afectados

BIG-IP (AAM, AFM, APM, ASM, Edge Gateway, FPS, LTM, Link Controller, PEM, WebAccelerator), versiones:

- 15.0.0, anteriores a 15.1.0
- 15.0.1, anteriores a 15.0.1.1
- 14.1.x, anteriores a 14.1.2.4
- 14.0.x, anteriores a 14.0.1.1
- 13.1.x, anteriores a 13.1.3.2

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://support.f5.com/csp/article/K12234501
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5883

CVE-2020-5888

Impacto

BIG-IP Virtual Edition (VE) puede exponer un mecanismo para que los atacantes de la red adyacente (capa 2) accedan a los demonios locales y eviten la configuración de bloqueo del puerto.

Los hosts en redes adyacentes pueden omitir la configuración de bloqueo de puertos en hosts BIG-IP VE.

Productos Afectados

BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM), versiones:

- 15.0.0, anteriores a 15.1.0.2
- 15.0.x, anteriores a 15.0.1.3
- 14.1.x, anteriores a 14.1.2.4

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://support.f5.com/csp/article/K73274382
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5888

CVE-2020-5876

Impacto

Existe una condición de carrera donde mcpd y otros procesos pueden realizar intentos de conexión sin cifrar a un nuevo par de sincronización de configuración. La condición de carrera puede ocurrir al cambiar la dirección IP de ConfigSync de un par, agregar un nuevo par o cuando se inicia por primera vez el Traffic Management Microkernel (TMM).

La condición de carrera ofrece una pequeña oportunidad para que un atacante tome el control de la conexión y falsifique un dispositivo de confianza para extraer y/o modificar información confidencial del sistema. Esta vulnerabilidad solo está presente cuando el sistema BIG-IP está configurado como parte de un grupo de dispositivos de alta disponibilidad (HA) ConfigSync.

Productos Afectados

BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM), versiones:

- 15.x, anteriores a 15.1.0
- 14.x, anteriores a 14.1.2.4
- 12.x, anteriores a 12.1.5.1

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://support.f5.com/csp/article/K32121038
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5876

CVE-2020-5884

Impacto

El modo de implementación predeterminado para la duplicación de pares de alta disponibilidad (HA) BIG-IP es inseguro. Este es un problema del plano de control que se expone solo en la red utilizada para la duplicación.

Los atacantes pueden leer y modificar datos en tránsito. Dependiendo de la implementación, esto puede incluir mensajes de reflejo de estado, detalles de conexión del cliente, paquetes de datos del cliente y / o datos de persistencia del cliente.

Productos Afectados

BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM), versiones:

- 15.0.0 - 15.1.0
- 14.1.0 - 14.1.2
- 13.1.0 – 13.1.3
- 12.1.0 – 12.1.5
- 11.6.1 - 11.6.5

Mitigación

Para mitigar esta vulnerabilidad, puede habilitar la variable de base de datos statemirror.secure para proteger la VLAN utilizada para duplicar entidades no confiables. Para hacerlo revisar el enlace en donde se detallan 2 procedimientos.

Enlace

https://support.f5.com/csp/article/K72540690

CVE-2020-5871

Impacto

ELas solicitudes no reveladas pueden conducir a una denegación de servicio (DoS) cuando se envían a servidores virtuales BIG-IP HTTP/2. El problema puede ocurrir cuando los cifrados, que han sido incluidos en la lista negra por HTTP/2 RFC, se usan en servidores de fondo. Este es un problema de plano de datos. No hay exposición en el plano de control.

Esta vulnerabilidad afecta solo al servidor virtual asociado con el perfil HTTP / 2 que tiene seleccionada la configuración del enrutador HTTP MRF. El sistema BIG-IP puede fallar temporalmente al procesar el tráfico a medida que se recupera de un reinicio de Traffic Management Microkernel (TMM). Si el sistema BIG-IP está configurado para alta disponibilidad (HA), fallará a un sistema par.

Productos Afectados

BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM), versiones:

- 14.1.0 – 14.1.2, versiones anteriores a 14.1.2.4

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://support.f5.com/csp/article/K43450419
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5871

CVE-2020-5887

Impacto

BIG-IP Virtual Edition (VE) puede exponer un mecanismo para que los atacantes remotos accedan a demonios locales y omitan la configuración de bloqueo de puertos.

La vulnerabilidad puede ocurrir en sistemas BIG-IP VE con la siguiente configuración:

- Un servidor virtual de reenvío IPv6
- Una dirección IP flotante de IPv6
- Un servidor virtual tiene el perfil HTTP configurado con proxy explícito http habilitado y un conjunto de manejo de conexión predeterminado para permitir

Los hosts en redes adyacentes pueden omitir la configuración de bloqueo de puertos en hosts BIG-IP VE.

Productos Afectados

BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator), versiones:

- 15.0.x, versiones anteriores a 15.1.0.2
- 14.1.0 – 14.1.2, versiones anteriores a 14.1.2.4

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://support.f5.com/csp/article/K10251014
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5887

CVE-2020-5879

Impacto

Bajo ciertas configuraciones, el sistema BIG-IP envía el tráfico del plano de datos a los servidores de fondo sin cifrar, incluso cuando se aplica un perfil SSL de servidor.

El sistema afectado envía algunas solicitudes al servidor de fondo sin cifrado, posiblemente con fugas de datos confidenciales. Las solicitudes afectadas por esta vulnerabilidad son procesadas por un servidor virtual asociado con un perfil DoS que tiene configurado un desafío CAPTCHA.

Productos Afectados

BIG-IP (ASM), versiones 11.6.1 - 11.6.5

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://support.f5.com/csp/article/K88474783
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5879

CVE-2020-5893

Impacto

Cuando un usuario se conecta a una VPN utilizando BIG-IP Edge Client a través de una red no segura, BIG-IP Edge Client responde a las solicitudes de autenticación a través de HTTP mientras envía sondas para la detección de portal cautivo.

Un atacante puede usar un ataque man-in-the-middle (MITM) mediante la implementación de un portal cautivo malicioso para explotar esta vulnerabilidad y obtener la respuesta de desafío de NT Lan Manager (NTLM) encriptada. Esto se puede usar para llevar a cabo ataques de diccionario de fuerza bruta o ataques de retransmisión NTLM si el atacante tiene acceso a la red de Active Directory.

Productos Afectados

APM Clients, versiones anteriores a 7.1.9

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://support.f5.com/csp/article/K97733133
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5893

CVE-2020-5890

Impacto

Al crear un QKView, las credenciales para vincular a los servidores LDAP utilizados para la autenticación remota de la interfaz administrativa BIG-IP no se ofuscarán completamente si contienen espacios en blanco.

El sistema BIG-IP puede revelar información confidencial utilizada para la autenticación con servidores LDAP (Lightweight Directory Access Protocol) a un usuario sin privilegios.

Productos Afectados

BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM), versiones:

- 15.x, anteriores a 15.1.0.2
- 14.x, anteriores a 14.1.2.4

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://support.f5.com/csp/article/K03318649
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5890

CVE-2020-5873

Impacto

Un usuario asociado con el rol de Administrador de recursos que tiene acceso a la utilidad de copia segura (scp) pero no tiene acceso a Advanced Shell (bash) puede ejecutar comandos arbitrarios utilizando una solicitud scp creada con fines malintencionados.

Un usuario autenticado con el rol de Administrador de recursos puede ejecutar comandos de shell con privilegios elevados.

Productos Afectados

BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM), versiones:

- 15.x, anteriores a 15.1.0
- 14.x, anteriores a 14.1.2.4
- 13.x, anteriores a 13.1.3.2
- 12.x, anteriores a 12.1.5.1
- 11.x, anteriores a 11.6.5.1

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://support.f5.com/csp/article/K03585731
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5873

CVE-2020-5872

Impacto

Al procesar el tráfico TLS con aceleración criptográfica de hardware habilitada en plataformas con hardware Intel QAT, el Microkernel de gestión de tráfico (TMM) puede dejar de responder y provocar un evento de conmutación por error.

La aceleración criptográfica de hardware falla y TMM puede dejar de responder, lo que provoca un evento de conmutación por error si el sistema BIG-IP está configurado como parte de un grupo de dispositivos. Esta vulnerabilidad se aplica a las siguientes plataformas:

- i4600, i4800, YK i4000
- i5600, i5800, HRC-i5000, HRC-i5800, i5820-DF
- i7600, i7800, i7000-D, i7820-DF
- i10600, i10800, i10000-D, HRC-i10800
- i11600, i11800, i11000-DS, i11000-D
- i15600, i15800, i15000-N
- VIPRION B4400N Blade

Productos Afectados

BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM), versiones:

- 15.x, anteriores a 15.1.0
- 14.x, anteriores a 14.1.2.4
- 13.x, anteriores a 13.1.3.2
- 12.x, anteriores a 12.1.5

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://support.f5.com/csp/article/K63558580
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5872

CVE-2020-5878

Impacto

Traffic Management Microkernel (TMM) puede reiniciarse en BIG-IP Virtual Edition (VE) mientras procesa tráfico IP inusual.

El sistema BIG-IP VE puede fallar temporalmente al procesar el tráfico cuando se recupera de un reinicio de TMM. Si el sistema BIG-IP VE está configurado para alta disponibilidad (HA), fallará a un sistema homólogo.

Productos Afectados

BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM), versiones:

- 15.1.0, anteriores a 15.1.0.2
- 15.0.x, anteriores a 15.0.1.2
- 14.x, anteriores a 14.1.2.4

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://support.f5.com/csp/article/K35750231
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5878

CVE-2020-5892

Impacto

Los componentes de BIG-IP Edge Client en BIG-IP APM, Edge Gateway y FirePass legacy permiten a los atacantes obtener la ID de sesión completa de la memoria del proceso.

Un atacante con privilegios locales suficientes en una máquina cliente que ejecuta Windows puede obtener acceso a la ID de sesión completa.

Nota: esta vulnerabilidad se limita al cliente BIG-IP Edge Client, F5 Access y FirePass heredado solo para Windows; no afecta el host BIG-IP o FirePass.

Productos Afectados

BIG-IP APM Clients, versiones anteriores a 7.1.9

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://support.f5.com/csp/article/K15838353
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5892

CVE-2020-5877

Impacto

La entrada con formato incorrecto al comando DATAGRAM :: tcp iRules dentro de un evento FLOW_INIT puede provocar una denegación de servicio.

Los atacantes remotos pueden realizar un ataque de denegación de servicio (DoS) en el sistema BIG-IP.

Productos Afectados

BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM), versiones:

- 15.x, anteriores a 15.1.0.2
- 14.x, anteriores a 14.1.2.4

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://support.f5.com/csp/article/K54200228
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5877

CVE-2020-5891

Impacto

Las solicitudes HTTP/2 no divulgadas pueden provocar una denegación de servicio cuando se envían a un servidor virtual configurado con la configuración de Fallback Host y un perfil HTTP/2 del lado del servidor.

El Microkernel de gestión de tráfico (TMM) puede generar un archivo central y reiniciarse, causando una interrupción del tráfico o un evento de conmutación por error. Esta vulnerabilidad solo afecta a los servidores virtuales con la configuración Fallback Host configurada y un perfil HTTP / 2 del lado del servidor asignado.

Productos Afectados

BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, FPS, Link Controller, PEM), versiones:

- 15.1.0, anteriores a 15.1.0.2
- 15.0.x, anteriores a 15.0.1.3
- 14.x, anteriores a 14.1.2.4

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://support.f5.com/csp/article/K58494243
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5891

CVE-2020-5881

Impacto

Cuando BIG-IP Virtual Edition (VE) está configurado con grupos de VLAN y hay dispositivos configurados con OSPF conectado a él, las interfaces de la Capa de abstracción de dispositivos de red (NDAL) pueden bloquearse y, a su vez, interrumpir la comunicación entre los procesos mcpd y tmm.

Este problema solo afecta a BIG-IP VE. El sistema BIG-IP no procesa temporalmente el tráfico a medida que se recupera de un reinicio de Traffic Management Microkernel (TMM), y los dispositivos configurados en un grupo de dispositivos pueden fallar.

Productos Afectados

BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM), versiones:

- 15.x, anteriores a 15.1.0.2
- 14.x, anteriores a 14.1.2.4
- 13.1.0 - 13.1.3

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://support.f5.com/csp/article/K03386032
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5881

CVE-2020-5886

Impacto

La configuración de los sistemas BIG-IP para la duplicación de conexiones en un par de alta disponibilidad (HA) transfiere objetos criptográficos sensibles a través de un canal de comunicaciones inseguro. Este es un problema del plano de control que se expone solo en la red utilizada para la duplicación de conexiones.

Los atacantes en ruta pueden leer y modificar los parámetros de Diffie-Hellman (DH) utilizados por los servidores virtuales habilitados para SSL/TLS en el plano de datos.

Productos Afectados

BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM), versiones:

- 15.x, anteriores a 15.1.0.2
- 14.x, anteriores a 14.1.2.4
- 13.1.0 – 13.1.3
- 12.1.0 - 12.1.5

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://support.f5.com/csp/article/K65720640
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5886

CVE-2020-5885

Impacto

Los sistemas BIG-IP configurados para la duplicación de conexiones en un par de alta disponibilidad (HA) transfieren objetos criptográficos sensibles a través de un canal de comunicaciones inseguro. Este es un problema del plano de control que se expone solo en la red utilizada para la duplicación de conexiones.

Los atacantes en ruta pueden leer y modificar las claves utilizadas para los conjuntos de cifrado basados en EXPORT.

Productos Afectados

BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM), versiones:

- 15.x, anteriores a 15.1.0.2
- 14.x, anteriores a 14.1.2.4
- 13.1.0 – 13.1.3
- 12.1.0 - 12.1.5

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://support.f5.com/csp/article/K17663061
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5885