Alerta de seguridad informática	9VSA-00093-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 de Diciembre de 2019
Última revisión	1 de Diciembre de 2019

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 diversas vulnerabilidades presentes en sus productos.

Vulnerabilidades

CVE-2019-6665
CVE-2019-6672
CVE-2019-6674
CVE-2019-6667
CVE-2019-6666
CVE-2019-6669
CVE-2019-6673
CVE-2019-6668
CVE-2019-6671

Vulnerabilidad

CVE-2019-6665

Impacto

Un atacante con acceso a la comunicación del dispositivo entre BIG-IP ASM Central Policy Builder y BIG-IQ / Enterprise Manager / F5 iWorkflow podrá configurar el proxy de la misma manera e interceptar el tráfico.

Con acceso al token de autenticación, el atacante podrá hacerse pasar por BIG-IP ASM Central Policy Builder y enviar datos de sugerencias corruptos o incorrectos al BIG-IQ / Enterprise Manager / F5 iWorkflow. Esto puede conducir a sugerencias de construcción de políticas incorrectas o una denegación de servicio parcial (DoS)

Productos Afectados

BIG-IP ASM, versiones:

- 15.0.0 – 15.0.1
- 14.1.0 – 14.1.2
- 14.0.0 – 14.0.1
- 13.1.0 – 13.1.3.1

Enterprise Manager, versión 3.1.1
BIG-IQ Centralized Management, versiones:

- 6.0.0
- 5.2.0 – 5.4.0

F5 iWorkflow, version 2.3.0

Mitigación

Aplicar las actualizaciones publicadas por el fabricante

Enlace

https://support.f5.com/csp/article/K26462555
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6665

Vulnerabilidad

CVE-2019-6672

Impacto

F5 BIG-IP AFM es propenso a una vulnerabilidad de denegación de servicio. Los atacantes pueden explotar este problema para causar una condición de denegación de servicio, negando el servicio a usuarios legítimos.

Productos Afectados

BIG-IP AFM, versiones:

- 15.0.0 – 15.0.1
- 14.1.0 – 14.1.2
- 13.1.0 - 13.1.3

Mitigación

Aplicar las actualizaciones publicadas por el fabricante

Enlace

https://support.f5.com/csp/article/K14703097
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6672

Vulnerabilidad

CVE-2019-6674

Impacto

F5 SSL Orchestrator es propenso a una vulnerabilidad de denegación de servicio. Un atacante puede explotar este problema para provocar condiciones de denegación de servicio.

Productos Afectados

F5 SSL Orchestrator, versiones:

- 15.0.0 – 15.0.1
- 14.1.0 – 14.1.2

Mitigación

Aplicar las actualizaciones publicadas por el fabricante

Enlace

https://support.f5.com/csp/article/K21135478
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6674

Vulnerabilidad

CVE-2019-6667

Impacto

F5 BIG-IP es propenso a una vulnerabilidad remota de denegación de servicio. Un atacante puede explotar este problema para provocar el agotamiento de los recursos que resulta en una condición de denegación de servicio.

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

- 15.0.0 – 15.0.1
- 14.1.0 – 14.0.0
- 13.0.0 – 13.1.1
- 12.1.0 – 12.1.4
- 11.5.1 – 11.6.5

Mitigación

Aplicar las actualizaciones publicadas por el fabricante

Enlace

https://support.f5.com/csp/article/K82781208
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6667

Vulnerabilidad

CVE-2019-6666

Impacto

Múltiples productos F5 BIG-IP son propensos a una vulnerabilidad de denegación de servicio. Los atacantes pueden explotar este problema para causar una condición de denegación de servicio.

Productos Afectados

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

- 15.0.0 – 15.0.1
- 14.1.0 – 14.0.0
- 13.0.0 - 13.1.1

Mitigación

Aplicar las actualizaciones publicadas por el fabricante

Enlace

https://support.f5.com/csp/article/K92411323
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6666

Vulnerabilidad

CVE-2019-6669

Impacto

F5 BIG-IP es propenso a una vulnerabilidad remota de denegación de servicio. Una explotación exitosa puede permitir que un atacante haga que se recargue el Microkernel de gestión de tráfico (TMM), negando el servicio a usuarios legítimos.

Productos Afectados

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

- 15.0.0 – 15.0.1
- 14.1.0 – 14.1.2
- 14.0.0 – 14.0.1

- 13.0.0 – 13.1.3
- 12.1.0 – 12.1.5
- 11.5.2 – 11.6.5

Mitigación

Aplicar las actualizaciones publicadas por el fabricante

Enlace

https://support.f5.com/csp/article/K11447758
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6669

Vulnerabilidad

CVE-2019-6673

Impacto

Múltiples productos F5 BIG-IP son propensos a una vulnerabilidad de denegación de servicio. Los atacantes pueden explotar este problema para causar una condición de denegación de servicio.

Productos Afectados

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

- 15.0.0 – 15.0.1
- 14.1.0 – 14.1.2

Mitigación

Aplicar las actualizaciones publicadas por el fabricante

Enlace

https://support.f5.com/csp/article/K81557381
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6673

Vulnerabilidad

CVE-2019-6668

Impacto

BIG-IP Edge Client para macOS puede permitir que usuarios sin privilegios accedan a archivos propiedad de la cuenta root

Productos Afectados

BIG-IP APM, versiones:

- 15.0.0 – 15.0.1
- 14.1.0
- 14.0.0
- 13.0.0 – 13.1.2
- 11.5.1 – 11.6.5

Mitigación

Aplicar las actualizaciones publicadas por el fabricante

Enlace

https://support.f5.com/csp/article/K49827114
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6668

Vulnerabilidad

CVE-2019-6671

Impacto

Múltiples productos F5 BIG-IP son propensos a una vulnerabilidad de denegación de servicio. Los atacantes pueden explotar este problema para causar una condición de denegación de servicio.

Productos Afectados

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

- 15.0.0 – 15.0.1
- 14.1.0 – 14.1.2
- 14.0.0 – 14.0.1

- 13.1.0 – 13.1.3

Mitigación

Aplicar las actualizaciones publicadas por el fabricante

Enlace

https://support.f5.com/csp/article/K39225055
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6671