Alerta de seguridad cibernética	9VSA20-00261-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Muy Alto
TLP	Blanco
Fecha de lanzamiento original	04 de julio de 2020
Última revisión	04 de julio 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 obtenida de F5 referente a una vulnerabilidad crítica de ejecución de código remoto (RCE) que afecta a la interfaz de gestión de tráfico o utilidad de configuración de usuario (TMUI).

Vulnerabilidades

CVE-2020-5902

CVE-2020-5902

Impacto

Esta vulnerabilidad permite a los atacantes no autenticados, o usuarios autenticados con acceso de red a TMUI, a través del puerto de administración BIG-IP o Self IPs, ejecutar comandos arbitrarios del sistema, crear o eliminar archivos, deshabilitar servicios y/o ejecutar arbitrariamente Código Java. Esta vulnerabilidad puede resultar en un compromiso completo del sistema. El sistema BIG-IP en modo Appliance también es vulnerable. Este problema no está expuesto en el plano de datos. El problema solo afecta el plano de control.

Productos Afectados

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

Versiones:

- 15.1.0 (Corrección introducida en versión: 15.1.0.4)
- 15.0.0 (Ninguna)
- 14.1.0-14.1.2 (Corrección introducida en versión: 14.1.2.6)
- 13.1.0-13.1.3 (Corrección introducida en versión: 13.1.3.4)
- 12.1.0-12.1.5 (Corrección introducida en versión: 12.1.5.2)
- 11.6.1-11.6.5 (Corrección introducida en versión: 11.6.5.2)

Mitigación

El proveedor indica que es posible eliminar la vulnerabilidad actualizando la versión con alguna de las versiones enumeradas anteriormente.

Si está utilizando los mercados de la nube pública (AWS, Azure, GCP y Alibaba) para implementar BIG-IP Virtual Edition (VE), F5 recomienda actualizar a las últimas versiones de BIG-IP que figuran en las correcciones introducidas en la columna sujeta a su disponibilidad en esos mercados.

Enlaces

https://support.f5.com/csp/article/K52145254
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5902